Secure Multimedia Controller 1.1

Fundamentals

Document Number: NN43001-325
Document Release: Standard 02.01
Date: February 2009

Produced in Canada

Revision history

February 2009

Standard 02.01. This document is up-issued to support Secure Multimedia Controller 2450 Release 1.1 and to address changes in technical content for SNMP support in SMC.

June 2007

Standard 01.02. Updated to reflect changes in technical content. Appendix B is updated to include Power consumption. Secure UNIStim Deployment chapter is updated with licensing information.

May 2007

Standard 01.01. This document is a new NTP. It was created to support a restructuring of the Documentation Library. This document is comprised of information on the Secure Multimedia Controller 2450 that was previously contained in the legacy document *Secure Multimedia Controller Implementation Guide* (553-3001-225), now retired.

May 2006

Standard 1.00. This document is a new NTP. It was created to support Secure Multimedia Controller 2450 Release 1.0.

Contents

New in this release

Secure Multimedia Controller Release 1.1 adds the following features and funtionality:

- IP Phone Call Recording. See “IP Phone Call Recording” on page 28.
- Active Call Failover. See “Support for CS 1000 Automatic Call Failover” on page 47
- Secure UNIStim graceful failover. See “Secure UNIStim graceful failover” on page 50.
- Firewall rules can be viewed and downloaded. See “Downloadable firewall rules from WebUI” on page 88.
- Custom protocols for IPsec traffic. See “IPsec traffic” on page 90.
- Extensible firewall rule templates. See “Extensible firewall rule templates” on page 90.

Introduction

This document is a global document. Contact your system supplier or your Nortel representative to verify that the hardware and software described are supported in your area.

Subject

This document describes Secure Multimedia Controller (SMC) 2450 Release 1.1 system architecture, software and hardware requirements, components, and network connections.

The SMC is one component of CS 1000 security. For further information on CS 1000 security, see *Security Management Fundamentals* (NN43001-604).

Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 and Nortel Multimedia Communication Server 5100 software. For more information, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

Applicable systems

This document applies to the following systems:

- Communication Server 1000E (CS 1000E)
- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)

- Communication Server 1000M Multi Group (CS 1000M MG)
- Multimedia Communication Server 5100 Server Micro System (V100)
- Multimedia Communication Server 5100 Server Simplex System (V100)
- Multimedia Communication Server 5100 Server Redundant System (V100)
- Multimedia Communication Server 5100 Server Large System (N240)

Intended audience

This document is intended for individuals responsible for installation, configuration, administration, and maintenance of the SMC 2450.

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (NN43011-220)
- *IP Line Fundamentals* (NN43100-500)
- *Security Management Fundamentals* (NN43001-604)
- *Communication Server 1000 Fault Management — SNMP* (NN43001-719)

Online

To access Nortel documentation online, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

CD-ROM

To obtain Nortel documentation on CD-ROM, contact your Nortel customer representative.

How to get help

This chapter explains how to get help for Nortel products and services.

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the telephone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also get help over the telephone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the telephone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Overview of the deployment process

Contents

This chapter contains information about the following topics:

Introduction

Before you deploy or upgrade an Secure Multimedia Controller (SMC), you need to understand the overall process. This chapter contains the high level information required to deploy a new system or a system upgrade.

Deploying a new system

Nortel recommends that you install a new SMC deployment through the following primary steps:

1 Install the SMC hardware. See “Hardware installation” on page 59.

2 Install and configure the SMC software. See “Installation and configuration” on page 97.

3 Incorporate the SMC into the network with the firewall unhooked (disabled) and UNIStim security turned off. All traffic passes through the box unhindered so that you can verify network connectivity. See “Firewall deployment” on page 77.

IMPORTANT!

If you encounter basic network connectivity problems during this step, verify the initial configuration of the SMC and the external routing of traffic through the SMC.

Ensure that the routes on the core intranet router are configured to send all Voice over IP (VoIP) traffic through the SMC and the VoIP equipment has the SMC interface designated as its default gateway.

4 Hook (enable) the firewall on the SMC and validate that baseline connectivity for back-end multimedia services(such as CS 1000, MCS, CallPilot, and Symposium) is not hindered. During this step, you can enhance and update the firewall rules to protect the devices in the secure multimedia zone. To ensure that packets do not drop due to incorrect firewall rules, view the firewall logs for events of dropped communication.

5 Turn on Secure UNIStim security for a subset of clients to troubleshoot UNIStim connectivity and populate the secure UNIStim server tables with the redirect information. See “Secure UNIStim deployment” on page 123.

WARNING

Prior to turning on UNIStim security, upgrade the image on all IP Phones that interface with servers that the SMC proxies. Prior to enabling UNIStim security, upgrade the firmware on all IP Phones that connect to CS 1000E and MCS 5100 systems behind the SMC.

6 Turn on Secure UNIStim for all IP Phones. See “Configuring the IP Phones” on page 142.

Description

Contents

This chapter contains information about the following topics:

Introduction

Multimedia infrastructure components are currently deployed in enterprise networks with desktop access to data and Voice over IP (VoIP)/Multimedia

Virtual LANs (VLAN). Desktop accessibility increases the vulnerability of these systems to internal threats, such as disgruntled employees, compromised systems, or infected laptops. Internal threats can be more severe than external threats for these critical infrastructure components. To provide adequate service availability, VoIP and other multimedia systems must be protected from internal threats.

The SMC 2450 is a security system that consists of a PC-based hardware platform with SMC software.

As shown in Figure 3 on page 30, the SMC 2450 creates a Secure Multimedia Zone (SMZ) between the enterprise Local Area Network (LAN)/Wide Area Network (WAN) and the Call Servers. The SMZ protects the signaling and media infrastructures of the MCS 5100 and CS 1000 product lines. All signaling and media traffic entering or leaving the SMZ must pass through the SMC.

The SMC is one component of CS 1000 security. For further information on CS 1000 security see *Security Management Fundamentals* (NN43001-604).

Release notes

To keep informed about SMC 2450 updates, refer to the release notes on the Nortel Web site. Using the My Notification feature, you can receive updates on the SMC 2450 by e-mail at the frequency you select.

Release note include information about:

- bug fixes
- enhancements
- known issues
- updated rules

For release notes, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

Key features

The SMC 2450 contains the following key features:

- Secure Multimedia Zones (SMZ)
- Secure UNIStim proxy
- High Availability (HA) configurations (active/standby)
- Administrative tools

The following sections describe these features in detail.

Security zones

Configuration of the SMC is built around the concept of multimedia security zones. A security zone is a protected subnet connected to the SMC through a port on the device. Multimedia infrastructure components, such as the signaling and media servers, are located in the zones. All traffic into and out of the zones flows through the multimedia controller. The SMC has six ports and supports up to four secure multimedia zones. The two remaining ports are used for management and intranet/untrusted traffic.

Two networks are mandatory in each SMC system installation:

- Management subnet: The management subnet transmits clustering and synchronization traffic between two SMC devices in a cluster. You can access the browser-based interface (BBI) through the management subnet.
- Intranet subnet: The intranet subnet represents the non-secure corporate intranet, which is the non-secure side of the SMC where the IP Phones generally reside.

Four optional primary subnets, referred to as secure multimedia zones (SMZ), interface with the SMC:

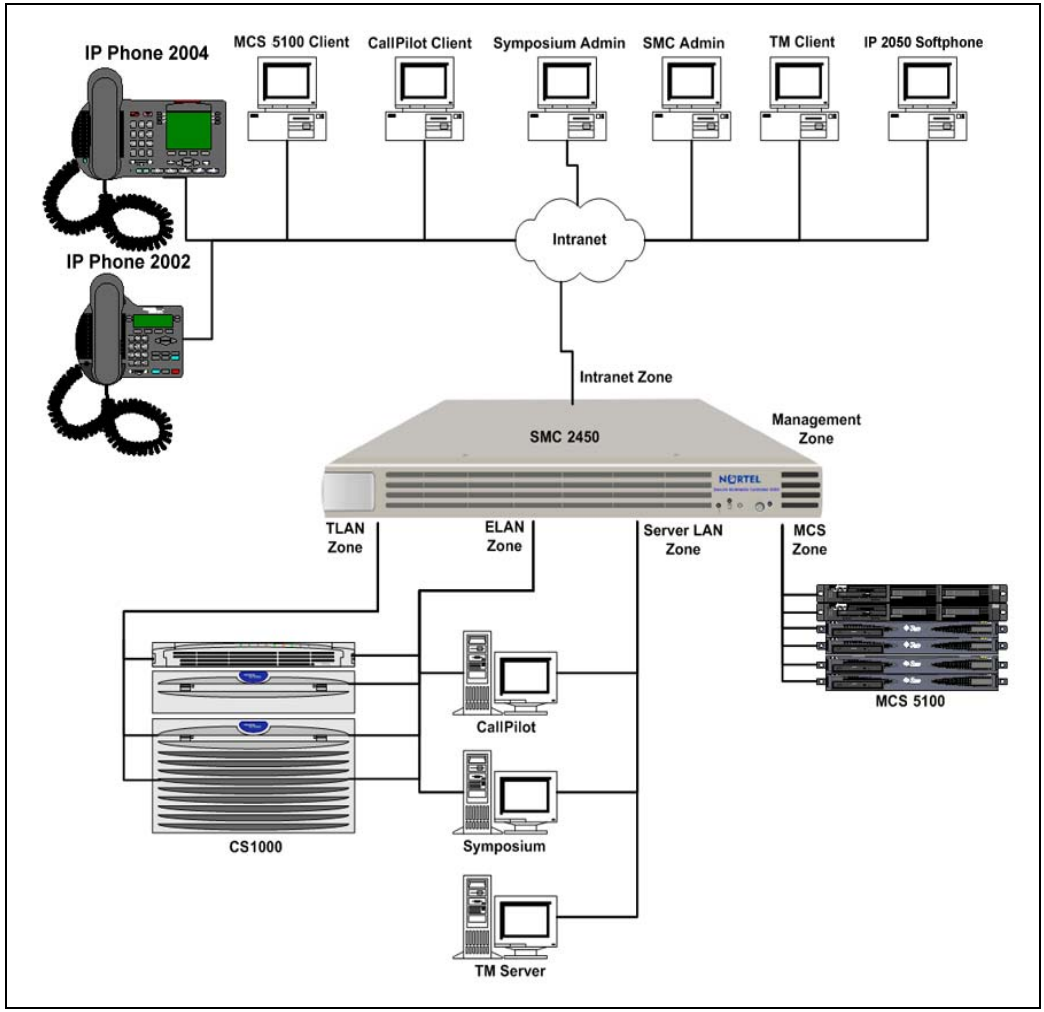
- ELAN subnet: The Embedded LAN (ELAN) subnet, which is the management LAN for CS 1000, isolates critical telephony signaling between the Call Server and other components.

- TLAN subnet: The Telephony LAN (TLAN) subnet, which is the voice LAN for CS 1000, carries telephony, voice, and signaling traffic to and from IP Phones and gateways.
- SLAN subnet: The Server Lan (SLAN), which serves the CS 1000, is the location of CallPilot, Symposium, and Telephony Manager.
- MCS LAN subnet: The Multimedia Communication Server LAN (MCS LAN) subnet is the location of the MCS suite of servers.

  Note: You can substitute the optional networks with user-defined networks.

Figure 1 on page 23 shows the basic subnet mappings available in the SMC.

Figure 1
Basic subnet mappings.



Management subnet

The management subnet is required on all SMC installations. It is a separate protected network that handles management, cluster, and synchronization traffic.

Management subnet configuration requires the following items:

- dedicated ethernet port on the SMC
- IP address for the management network interface (one for each SMC in a High Available (HA) configuration)
- subnet mask (the management subnet requires a mask that supports at least two addresses for a stand-alone system)
- cluster Management IP address (MIP) (a virtual address used on a single SMC or shared through Virtual Router Redundancy Protocol (VRRP) with both SMCs in a HA configuration)
- a cross-over cable to connect the management ports in a HA configuration

Management IP address

A single cluster MIP address is shared by the master SMC and the backup SMC in HA scenarios. The cluster MIP address is hosted on the master SMC and migrates to the backup SMC if the master fails to operate. The cluster MIP address is also required for a stand-alone configuration.

Intranet subnet

The intranet defines the untrusted networks on which the IP Phones reside. All traffic into the secured multimedia zones originating from the intranet passes through the SMC for stateful filtering, rate limiting, attack protection, and the secure UNIStim proxy support.

The intranet setup requires the following items:

- dedicated port on the SMC
- IP address for each SMC in a HA configuration
- virtual IP address for the HA configuration

- subnet mask

Secure multimedia zones

Up to four user-defined SMZs can exist for each SMC stand-alone device or HA cluster. Each zone is protected by a customizable stateful packet filter.

Zone configuration

Setup of an SMZ requires the following parameters:

- descriptive name
- dedicated ethernet port
- network interface IP address
- subnet mask
- additional IP address and VRRP virtual IP address for HA configurations

Inbound/outbound access rules

The administrator specifies inbound access control rules for traffic that originates in the intranet and flows into a security zone, and outbound access control rules for traffic that exits a security zone and flows out to the intranet.

Configure inbound and outbound access rules separately. Each rule contains the following parameters:

- the source and destination IP address for the traffic
- the service, such as a protocol or a list of port ranges, against which the packets are matched
- whether the traffic is allowed or denied
- flow control parameters

Automatic rule generation

The SMC can automatically generate rules to protect traffic flowing into the SMZs from the intranet. Rule sets are supported for the following subnets:

- ELAN subnet, which protects the trusted management network of the CS 1000, requires the highest security

- TLAN subnet, which consists of packets to the Signaling Servers, Media Gateways, and other applications
- Server LAN, which hosts applications that work in tandem with the CS 1000 devices such as CallPilot, Symposium, and Telephony Manager (TM)
- MCS LAN, which protects the suite of MCS products

Note: Traffic flowing from TLAN to MCS LAN is subjected to an outbound TLAN policy and then an inbound MCS LAN policy.

The administrator can customize and configure the rules in each SMZ. For example, the administrator can add and delete custom rules, and apply multiple rule sets to a single SMZ.

IMPORTANT!

See the release notes for recommendations for how to allocate the subnets to specific Nortel products.

For release notes, click the Technical Documentation link under Support & Training on the Nortel home page:

www.nortel.com

External routing updates

The SMC, a Layer 3 device, must be installed within the path of all traffic between the intranet and the SMZs for both the CS 1000 and MCS configurations. To route traffic through the SMC on its way to or from the

protected domain, you need to modify the routing tables for devices on both sides of the SMC

IMPORTANT!

When integrating the SMC into an existing network, you can encounter routing issues. VoIP equipment must have the SMC as the primary gateway. Configure the intranet core router to send all VoIP traffic through the SMC.

The main router on the intranet side requires static routes for each of the subnets protected by the SMC. The main router can use OSPF to broadcast these routes and enable client connectivity.

SMC static routing updates

The SMC has a default single gateway, which is expected to be in the intranet. Each security zone is, by default, comprised of a subnet defined by a subnet mask. If the security zone consists of numerous subnets, add a static route to the SMC to route traffic to the subnets. The route specifies a gateway within the subnets, such as the ELAN subnet or TLAN subnet, through which traffic must be routed.

IMPORTANT!

The SMC supports a single default gateway; it does not support dynamic routing protocols such as Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) protocols.

Network integration

Prior to deploying the SMC, all devices on each subnet must be connected to a Layer 2 switch. The SMC does not support Virtual LANS (VLAN); therefore, a single network interface is required for each subnet.

In VLAN networks, multiple devices are connected across routes but are part of the same subnet. Update these networks to identify the switch as the primary interface through the SMC.

In a standard CS 1000 installation, the SMC is in the path of traffic between the Intranet and the protected subnets so that all traffic flows through the SMC.

IP Phone Call Recording

A phone conversation made from an IP Phone can be recorded on a standalone recording device by simply pushing a button on the IP Phone. When the button is pushed to start recording, the IP Phone begins to transmit a duplicate media stream to the recording device. The original media stream carries the voice conversation.

The recording device may be located inside or outside of the Secure Multimedia Zone (SMZ). The IP address and the port number of the recording device are dynamic. The Signaling Server communicates the IP address of the recording device to the IP Phone in a UNIStim message.

The Signaling Server uses UNIStim messages to instruct an IP Phone to start and stop IP Phone Call Recording. During runtime, if the SMC detects that the recording device is located within the SMZ, the SMC Secure UNIStim Proxy can dynamically update the firewall rules to open a pinhole for the duration of the recorded call. The SMC provides a Port Lifetime for the firewall pinhole. If a UNIStim Stop Call Recording message is not received, the firewall pinhole is closed after the expiration of the Port Lifetime.

IP connectivity

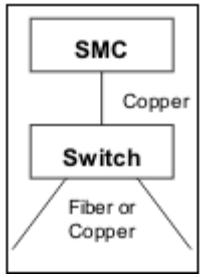
LAN ports

The SMC supports six 10/100/1000 Base TX (copper) ports. Each port must be on a separate subnet and the management and intranet networks must always be present.

For integration of the SMC into optical networks or MultiLink Trunking (MLT) networks in which more than a single port is used for a logical trunk, an additional switch device is required to work in tandem with the SMC. The switch interfaces with the SMC using a copper port and employs additional ports on the switch for either the fiber interface conversion or multiplexing.

In this type of configuration, consider the additional switch and the SMC to be a single unit. If either the switch or the SMC fails, it is comparable to a single SMC device failure.

Figure 2
SMC cabling



This document does not provide information about third-party media conversion devices that convert signals between copper and fiber.

SMC configurations

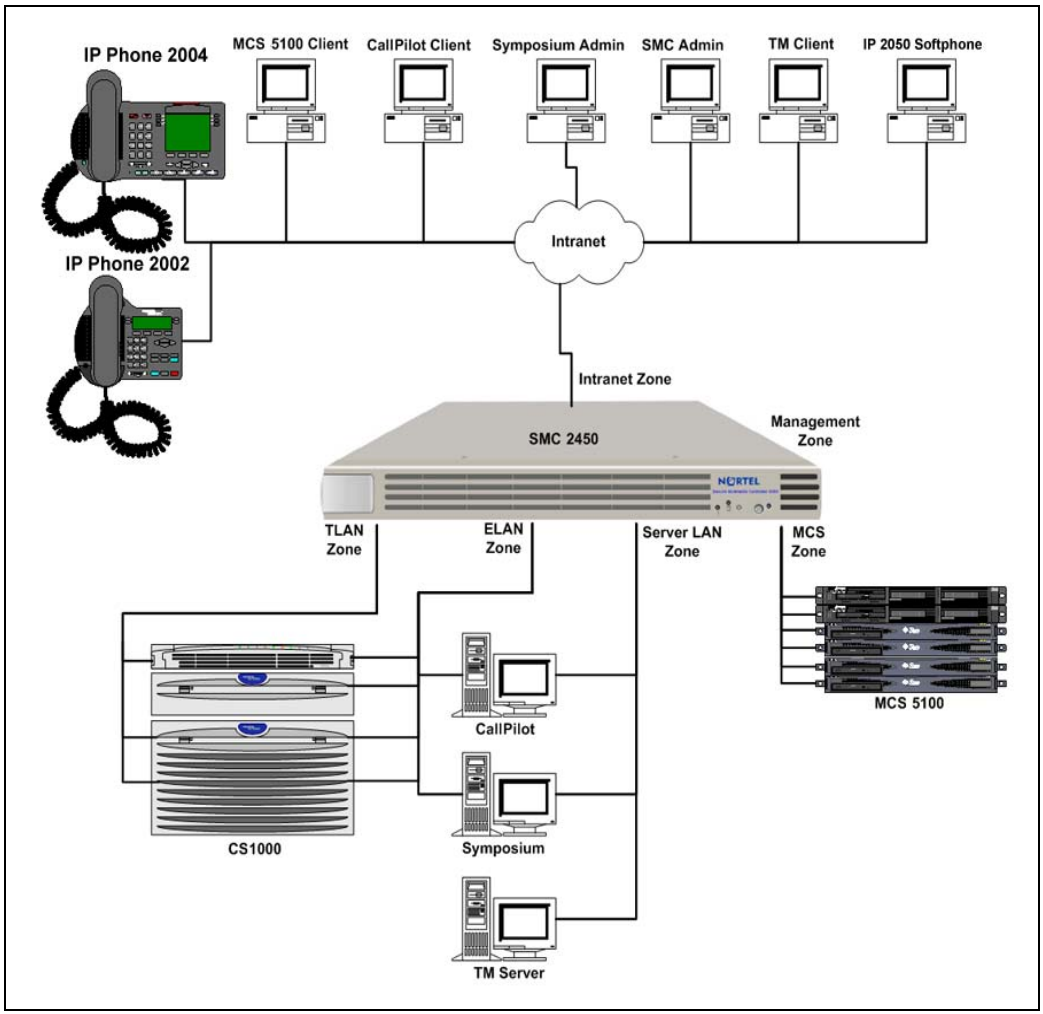
The SMC supports two types of configurations:

- Stand-alone
- High Availability (HA)

Stand-alone configuration

The stand-alone configuration contains a management network, intranet network, and one or more security zones. Each of the SMZ networks requires a unique port on the SMC device and an IP address. Figure 3 on page 30 illustrates a typical CS 100 topology

Figure 3
Stand-alone configuration



The management network needs two IP addresses in the stand-alone configuration. The first address is the host IP address, which is the IP address for the SMC. The second IP address is the cluster Management IP (MIP) address. Users communicate with the SMC using the cluster MIP address.

The host IP address and the cluster MIP address must reside in the same subnet.

IMPORTANT!

In a stand-alone configuration, the equipment residing on the Secure Multimedia Zones uses the SMC network interface IP addresses as their gateway address. For example, a CS 1000 Signaling Server TLAN Gateway IP address is the SMC TLAN IP address

High Availability (HA) configuration

In the HA configuration, each security zone requires three IP addresses: one IP address for each physical SMC network interface and a Virtual Router Redundancy Protocol (VRRP) address. The VRRP address is hosted by the VRRP master and floats to the backup if the master fails. Figure 4 on page 32 illustrates a typical SMC HA configuration.

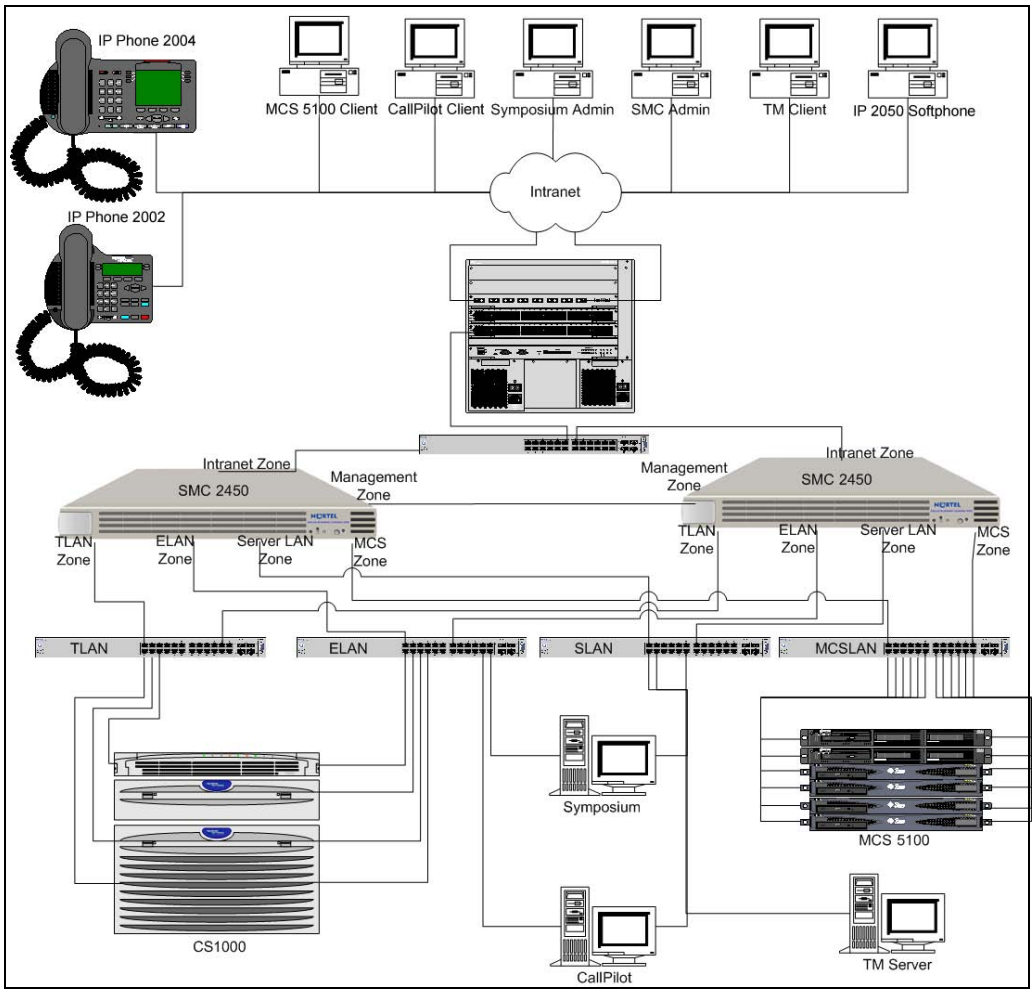
IMPORTANT!

In a High Availability configuration, the equipment residing on the Secure Multimedia Zones uses the SMC Virtual IP addresses as their gateway address.; for example, a CS 1000 Signaling Server TLAN Gateway.

When upgrading from a stand-alone SMC to a High Availability SMC installation, review carefully the IP addressing scheme so that the equipment in the Secure Multimedia Zones do not need the gateway IP addresses changed.

For example, when upgrading from stand-alone to High Availability configuration, change the IP addressing so the existing SMC network interface IP addresses are used as the Virtual IP addresses when the HA configuration is implemented.

Figure 4
High Availability configuration



VRRP IP addressing

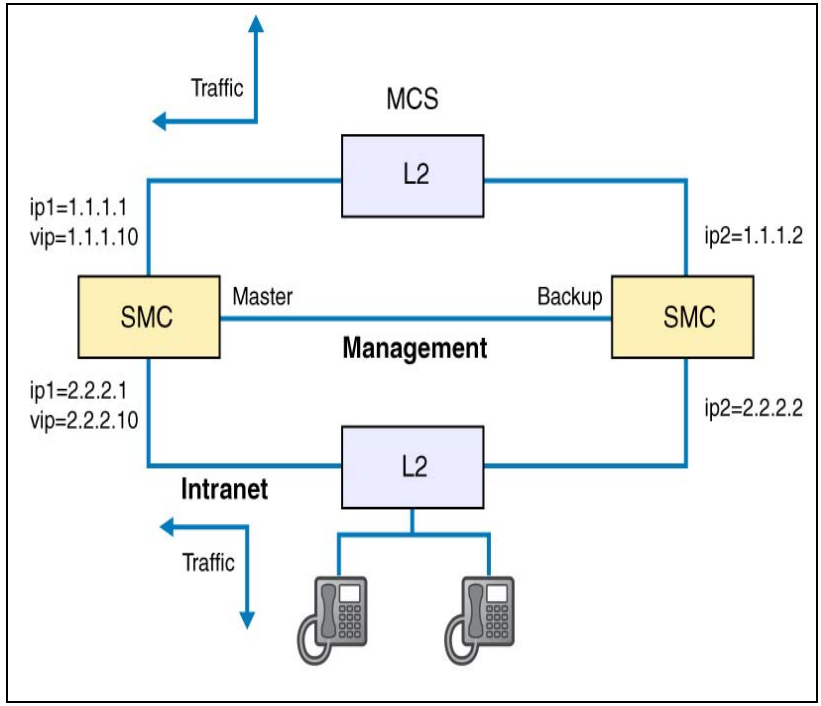
A High Availability cluster consists of two SMC devices: one SMC acts as the active device and the other acts as the backup device. In this scenario, only one SMC processes traffic. If the active SMC fails, all traffic is redirected to the backup SMC, which becomes active. SMC uses Virtual Router

Redundancy Protocol (VRRP) to determine which device is the master. The other device, by default, is the backup.

As shown in Figure 5 on page 33, VRRP requires three IP addresses for each cluster interface:

- two real IP addresses: one for each SMC in the cluster
- a floating IP address owned by the master SMC

Figure 5
VRRP IP addressing



In all routing tables in external devices, use the floating IP address to route packets. The floating IP address is always available even when one SMC in the cluster fails.

State synchronization

To allow for faster connection re-establishment during a failover, the Secure UNIStim proxy master key is synchronized across both SMCs in the HA configuration. Master keys are also persistently stored on disk.

Traffic protection

The SMZ provides stateful filtering and Denial of Service (DoS) attack protection on all packets that flow through it.

Stateful filtering

A stateful filter protects services running in the SMZ by using automatically generated access control lists and filtering policies. Administrators can customize these lists to handle all traffic that originates or terminates on the multimedia devices.

Stateful filtering is more secure than a simple packet filtering in that stateful filtering keeps track of the protocol's state in every session, thus ensuring that the stateful filtering device can:

- differentiate between a UNIStim IP Phone and server in a conversation
- detect the direction of traffic
- detect non-compliant state changes

DoS attack protection

An embedded DoS Defense Engine protects against common DoS and Distributed DoS (DDoS) attacks. The SMC provides flow control and rate-limiting features, which are tied to stateful filtering policies.

Rate limiting

You can use rate limiting to protect services in the Multimedia Zone (MMZ) by bounding the number of connections, bytes, or packets per second in each signaling channel (such as for UNIStim, H.323, and SIP).

Media stateful filter

The SMC acts as a stateful filter for Real-time Transport Protocol (RTP) media traffic. The SMC protects the Media Gateways from attacks, such as User Datagram Protocol (UDP) floods. To protect the gateways, the SMC lets a media stream come into the SMZ only if the gateway initiated a stream going out first.

Secure UNIStim proxy

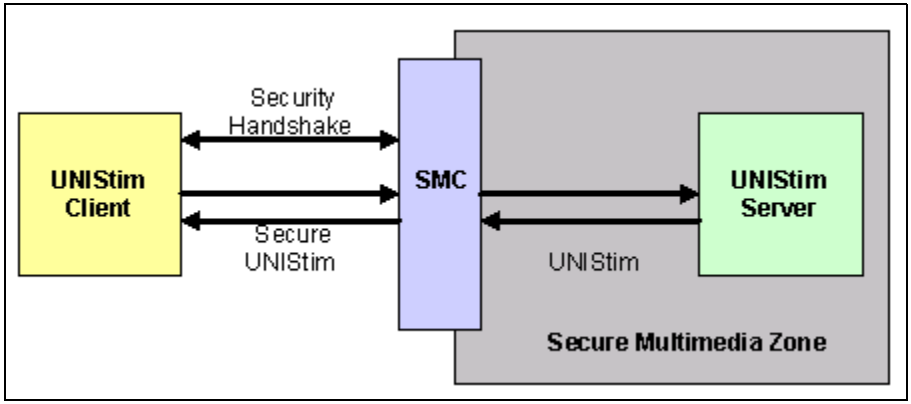
UNIStim is a Nortel-proprietary signaling protocol used within the MCS and CS 1000 product lines; however, the first release of the SMC supports only CS 1000. Using UNIStim, a UNIStim IP Phone communicates with a UNIStim server (TPS) using the User Datagram Protocol (UDP). The SMC Secure UNIStim proxy provides the following functionality:

- Secure UNIStim support
- transparent proxy support
- granular policies
- key management

Secure UNIStim support

The transparent UNIStim security proxy within the SMC enables UNIStim IP Phones to communicate with insecure UNIStim servers in a protected fashion, with encryption terminated at the SMC before the unencrypted traffic is passed to the back-end server. Nortel recommends that you install the SMC in close proximity to the server to minimize the exposure of insecure traffic.

Figure 6
Secure UNIStim proxy



UNIStim security enhances the basic UNIStim protocol by providing Advance Encryption Standard (AES) 128-bit encryption for confidentiality and an AES-based Message Authentication Code for authentication and integrity.

Transparent proxy support

Because the SMC is a transparent proxy, the clients communicate directly to the UNIStim Signaling Servers. The clients have no knowledge that the SMC is inserted itself between the server and client, and intercepting the signaling traffic.

Granular policies

Administrators can specify granular Secure UNIStim policies for individual hosts or subnets. These granular policies allow administrators to define whether particular clients require a Secure UNIStim connection, an upgrade to Secure UNIStim, or both. The policies also specify how often encryption keys used in the communication are renewed.

UNIStim policies

UNIStim policies determine whether:

- a Secure UNIStim connection is required for traffic to traverse the SMC
- the SMC can update an insecure UNIStim connection to use Secure UNIStim

The administrator can specify the UNIStim policy filtering based on the subnet of the client.

Key management

The SMC generates, imports, and exports RSA keys used for Secure UNIStim. Table 1 on page 38 identifies the three RSA key types.

> ***Note:*** Rivest, Shamir, and Adleman (RSA) is the algorithm used as a public key cryptography system employed in both encryption and authentication.

Comparison of the public and private keys

The private key is 1024-bit RSA key that is associated with a unique public key that is sent to the clients. The private key is stored securely on the SMC, whereas the public key is sent out to the IP Phones over an insecure channel and is used to encrypt the master fingerprint that is employed later in the Secure UNIStim handshake.

Key fingerprint

The key fingerprint is a 16-character string that represents a hash or digest of the public key. When an IP Phone receives the public key from the SMC during the Secure UNIStim handshake, the key fingerprint stored on the IP Phone is compared with the public key to ensure a match. The key fingerprint

is unique to the public key and the public key to key fingerprint match authenticates the SMC to the IP Phone.

IMPORTANT!

Public key fingerprints are currently exported as both 16- and 32-character hexadecimal strings; however, only the 16-character string is currently employed to configure the IP Phones.

Examples:
16 characters: 9d581d2cca15141b
32 characters: 9d581d2cca15141b80623a942a59d7d3

Table 1
RSA key types

Key	Description
Server private key	The SMC maintains a 1024-bit RSA private key, which is used to initiate the secure UNIStim key exchange. After the UNIStim IP Phone sends the initial "Hello" message to the SMC, the SMC responds by sending the public key to the IP Phone. The IP Phone then generates a fingerprint of the public key and compares the result to the public key fingerprint entered into the UNIStim IP Phone by the user. If they match, the UNIStim IP Phone is assured it is talking to the correct server.

Table 1
RSA key types

Key	Description
Master key	The master key is generated by the UNIStim IP Phone, encrypted with the server's public key, and returned to the server. The master key is stored on both the UNIStim IP Phone and server. It is used to create two unique session keys: one for encryption, and one for authentication.
Session keys	All secure UNIStim packets are encrypted with one session key and authenticated with a second. Each session key is derived independently on the UNIStim IP Phone and server using the master key along with parameters passed during connection initiation. Because session keys are used for every packet sent, Nortel recommends you regenerate the session keys periodically.

Dynamic Host Configuration Protocol

The IP Phones can use a static IP address or use full or partial Dynamic Host Configuration Protocol (DHCP) to acquire its own IP address and the IP address of the Terminal Proxy Server (TPS) in CS 1000 setups. The TPS represents the server side of the UNIStim protocol. DHCP can also provide the UNIStim IP Phone with a security-enabled Action Byte, which forces the IP Phone to initiate the UNIStim connection using the secure handshake.

Note: Phase 2 IP Phones can have more than one fingerprint stored at a time.

Automatic client fingerprint update

If an IP Phone runs firmware that supports secure UNIStim but does not have a primary key fingerprint, the SMC can automatically update the fingerprint to the IP Phone.

Please note that this is a restricted feature. The following conditions must be met:

- The IP Phone firmware must support Secure UNIStim. If not, you must update the firmware prior to using this feature.
- The IP Phone must not already have a primary key (both S1 and S2 keys must be blank, or each must contain 16 'f's). If it has, the autoload does not work again. This limitation minimizes security risks.
- The IP Phone must first connect in non-secure mode.
- You must configure the IP Phone policy in the Web UI to allow Secure UNIStim upgrades.

After successful connection, check IP Phone primary key configuration to ensure the primary key is loaded. See “Private key updates” on page 159.

Session caching

The SMC supports session caching, which enhances the performance of the IP Phone handshake. When the UNIStim IP Phone logs in a second time, the server reuses the previous master key and session to create a new session key. This prevents the TPS from generating another master key. Session caching is enabled as part of the UNIStim policy.

Administrative tools

You can manage the SMC using the following administrative tools:

- Web User Interface (Web UI)
- Command Line Interface (CLI)

Note: The CLI must be used for initial configuration. Most tasks, other than initial configuration, are supported by the Web UI and the CLI. However, ease of use makes the Web UI the preferred administration tool.

Web User Interface (UI)

SMC 2450 supports Web UI, a web-based graphical user interface (GUI) that offers an alternative to the command line interface (CLI). Web UI

management simplifies overall management of features like granular policies and key management.

Traditional command line interface (CLI)

SMC 2450 supports traditional CLIs. See “The Command Line Interface (CLI)” on page 187.

SNMP support in SMC

Overview

The Simple Network Management Protocol (SNMP) agent in SMC supports all three versions of the SNMP security model: v1, v2c and v3 (USM). SNMPv3 is recommended as it provides enhanced security, such as authorization and privacy. For further information on SNMP capabilities in a CS 1000 system see *Communication Server 1000 Fault Management — SNMP* (NN43001-719).

Supported MIBs

SMC supports the following Management Information Bases (MIB):

- alteon_smc.mib
- altroot.mib
- ALTEON-ISD-PLATFORM-MIB.mib

To download an MIB from the SMC Web UI, navigate to the **Administration > SNMP > MIBs** page. The Web UI lists the MIBs available on SMC and provides options to download them.

Configuring SNMP

The SNMP configuration options are provided in the Web UI **Administration > SNMP** menu. The SNMP configuration pages include:

- General Settings
- System Settings
- SNMP Trap Hosts

- USM Users
- Advanced Settings

i. **General Settings**: The following general SNMP configuration options are provided in this page:

– Status: Option to enable or disable the SNMP support.

– Security Model: Option to specify the SNMP security model (v1, v2c or v3) to be used.

– SNMP Access Control: Option to enable/disable the SNMP access control.

– Events/Alarms: Options to enable/disable sending of cluster events and alarms to the configured SNMP trap hosts.

– SNMPv1/v2c Options: The administrator can configure the read community string for SNMPv1/v2c access.

– SNMPv3 (USM) Options: The administrator can specify the desired degree of SNMP USM security.

ii. **System Settings:** Options to configure the parameters in the standard SNMPv2 MIB for the system. The parameters that can be configured are: Email Contact, Cluster Name and Cluster Location.

iii. **SNMP Trap Hosts**: The hosts to which the SNMP events and alarms are to be sent must be configured in the **SNMP Trap Hosts** page. The page lists the currently configured trap hosts and allows the administrator to add new hosts. The following options should be specified while adding new trap hosts:

– IP address of the trap host.

– Port to which trap should be sent (SNMP default is 162).

– Community string for the trap host.

– In the case of SNMPv3, the user employed for trap authentication. The user must exist in the administration database and can belong to either the "oper" or "admin" groups. The "oper" group is recommended. The authentication and encryption passwords are the same as those currently in the database.

iv. USM Users: This page allows the administrator to configure the users employed in SNMPv3 (USM) authentication/ encryption. This user table is entirely separate from the global administration user database and is used only in SNMPv3 requests. The page lists the currently configured users, and provides an option to add new users. The following options should be specified while adding new users:

– Name of the user for SNMPv3 (USM) authentication/ encryption.

– Type of permission allowed for the user (read and/or trap).

– Password used in MD5 authentication. This must be set when the user is created.

– Password used in DES encryption. This must be set when the user is created, even if privacy is not desired.

v. Advanced Settings: This page allows the administrator to configure the source IP to be used for SNMP traps generated by SMC. The following options are available:

– auto: Use the IP address of the outgoing interface. This is the default..

– unique: Use the IP address of the SMC management port.

– MIP: Use the cluster Management IP (MIP) address. This setting is useful with applications that expect devices to be limited to only one IP address, such as some versions of HP OpenView.

Other supported administrative tools and features

SMC 2450 supports the following administrative tools and features:

- **Logging.** The SMC supports local system logging, remote system logging, and log archiving. Logs detailing security issues and violations automatically are generated for the stateful filter and Secure UNIStim proxy.
- **Role-based administration.** Two primary management roles exist on the SMC: administrators and operators. Administrators can add and delete users, modify all aspects of the configuration, and update the software. Operators have read-only access to the configuration and performance data. For more information about roles, see "Users and passwords" on page 166.
- **RADIUS authorization.** Radius can be used in the enterprise environment for server access control. Administrator credentials can be stored on the SMC or on a RADIUS server.
- **RADIUS accounting.** The SMC can maintain a log of configuration user accesses and modifications, and direct this data to a RADIUS accounting server.
- **Maintenance dump.** The SMC supports maintenance dump functionality, which you can configure to automatically generate a compressed file that includes relevant logs, configuration, and statistics. Administrators can download this file using the Web UI or CLI and provide it to Nortel support personnel.

Resiliency

Communications reliability is critical to the operation of any business. The Secure Multimedia Controller (SMC) system provides several levels of redundancy to ensure that the telephony services can withstand single hardware failures.

SMC resiliency features

Active-standby configuration

In an active-standby configuration, the active SMC handles all traffic, and the backup SMC takes over if the active SMC fails. VRRP is used to determine the failover and is able to determine network loss in a matter of seconds.

Session cache synchronization

An initial secure UNIStim handshake requires high SMC CPU resource utilization. Using the session cache synchronization feature, an IP Phone can reconnect and establish a secure connection with much less CPU resource usage.

The session cache synchronization feature sends the session cache information from the master SMC to the backup SMC in real-time; thereby allowing for a quick re-establishment of connectivity on a failover.

TCP Failover and Port Bypass

Nortel VoIP solutions utilize both TCP and UDP as the primary transport protocols for various applications. TCP is used by applications such as H.323 (H.225 and H.245), used for communication between the SIP Proxy Server (SPS) and the Call Server, and used for MeetMe conferences.

When an SMC failover occurs, all data is redirected to the new master SMC, which does not maintain the current TCP session details. Therefore, the SMC stateful firewall drops the data packets associated with the TCP sessions, resulting in session failure.

In most failure situations, a new TCP session is not established until the SMC closes the original session on the old master SMC, or when the TCP end point detects the failure and attempts to re-establish the session. The resulting downtime can take 15 minutes.

To maintain continued TCP service when the SMC failover occurs, Nortel recommends that you create a Port Bypass. The Port Bypass feature allows all traffic destined to, or originating from, a particular port to flow through the SMC, but bypass the stateful firewall layer.

If you select service H323 (or H_323) on any of the secure interfaces such as ELAN and TLAN, then ports 1719 and 1720 are automatically added to the port bypass list.

> ***Note:*** Traffic against ports on the Port Bypass list is not protected by SMC.

VoIP equipment failure

In general, the SMC does not affect standard failure scenarios, such as Call Server and Signaling Server failures, within the CS 1000 or MCS product suites, as long as the traffic continues to flow through the master SMC. The failover scenarios and the activity of the current telephone call is the same as if the SMC were not present.

Branch office failover scenario

In this scenario, an IP Phone 2004 is using a Signaling Server at the main office and the WAN connection goes down. Both the main office and the branch office are protected by an SMC device.

The speech path is lost as soon as the network connection goes down.

The IP Phone reboots and re-registers with the Signaling Server at the branch office. During the reregistration, the IP Phone needs to create a secure session with the SMC at the branch office.

IMPORTANT!

In a branch office failover scenario, one UNIStim Phone can be redirected to register securely with different Call Servers behind multiple SMCs. Provide all SMCs with the same RSA key to avoid a security error. Encrypt the key with a password and export it from a primary SMC. See “Exporting the private key” on page 152. Then import the key into the other SMCs and set it to be the primary key.

SMC standalone failure

The SMC is a Layer 3 device. The failure of a single SMC that is not part of a High Availability configuration drops all packets directed to it, thereby effectively blocking connectivity.

IMPORTANT!

Nortel recommends that you install a High Availability cluster in all critical SMC installations.

Support for CS 1000 Automatic Call Failover

Automatic Call Failover (ACF) is a Communication Server 1000 (CS 1000) feature that

- enables IP Phones to maintain active calls, even after the IP Phones detect that connectivity to the Signaling Server (such as the CS 1000 Signaling Server) has been lost
- enables IP Phones to attempt connection to the alternate Signaling Server (such as the CS 1000 Signaling Server) in the background. For ACF to be fully functional, it requires all the VoIP entities, such as the Call Server, Signaling Server, and the IP Phone firmware to support ACF.

CS 1000 ACF is not supported in SMC Release 1.0. In an environment where an SMC 2450 is part of the topology, SMC Release 1.1 must be installed if the ACF feature is required.

There is no specufic user provisioning required on SMC to turn on this feature.

Campus redundancy

The Nortel Communications Server (CS) 1000 system is a highly-scalable and robust IP PBX that offers support of IP-based applications using industry-standard interfaces, while providing an industry-leading set of telephony features and applications.

Using the campus redundancy feature, you can separate the CS 1000 Call Servers in a campus environment for "campus mirroring". This feature connects two Call Servers, one active and one redundant, through an Ethernet network interface. Call processing is switched over gracefully between the two CPUs without interrupting ongoing calls and registered IP Phones.

To help eliminate any potential system down time, configure a pair of CS 1000 CPUs to form a completely redundant IP telephony network. You can install the following equipment as redundant systems:

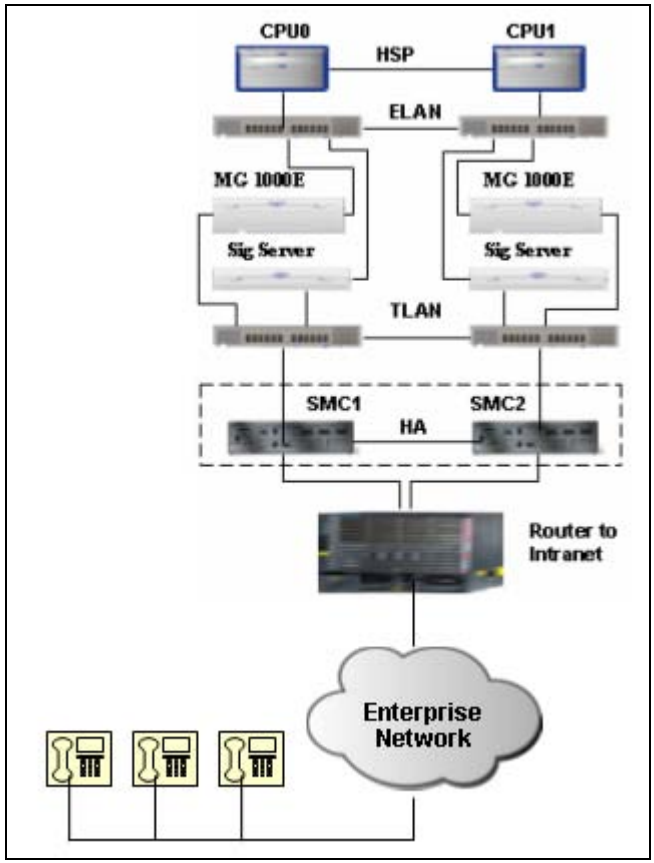
- Signaling Servers
- TLAN and Layer 2switches
- Layer 3 routers

Before placing an SMC system into a campus redundancy environment, consider that a minimum alternation of the existing data/voice network must not degrade the existing VoIP functionalities and must fully comply with the existing redundant network layout with SMC High Availability (HA) support.

SMC deployment with campus redundancy

Figure 7 on page 49 illustrates the general location of the SMCs in a campus redundant environment. The two SMCs form a High Availability cluster, consisting of an active and a backup device. Graceful switchover of the CS 1000 is fully supported.

Figure 7
SMC campus redundancy



Requirements and recommendations

No special configuration is required on the SMC to support campus redundancy; however, additional system-wide configuration changes are required to deploy the SMC system into the campus redundant environment:

- To avoid potential routing problems, IP addresses from the same subnet must be assigned to the SMCs connected to the two different TLAN switches. This requirement complies with the CS 1000 requirement when configuring a Campus Redundant IP telephony network.
- The Virtual Router IP address configured for the SMC HA TLAN interface must be the default gateway for all the Signaling Servers. Without SMC, the default gateway for these devices is the upper interface IP address of the router to the intranet.
- To route packets properly to the CS 1000 devices, the router must use the Virtual Router IP address of the SMC intranet interface as the gateway IP address.
- The SMC, as a router, can impact IP address assignments for devices on both sides of the SMC. Note that this is also true for SMC integration into non-campus redundant configurations.

Secure UNIStim graceful failover

SMC Release 1.1 supports graceful failover. Failure of the Master SMC in a cluster, or failure of the Layer 2 device attached to the Master SMC, does not impact end users. If the Master SMC in a cluster fails, or if the Layer 2 device attached to the Master SMC fails, registered IP Phones are gracefully switched to the Backup SMC.

SMC Release 1.0 does not support graceful failover.

> ***Note:*** The Secure UNIStim Graceful Failover does not address the TCP failure as described in "TCP Failover and Port Bypass" on page 45. To address the TCP failure when SMC failover occurs, use the Port Bypass feature.

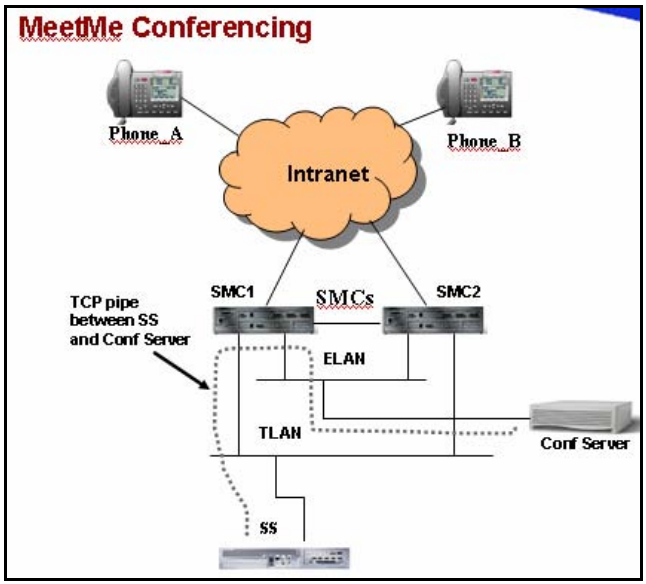
Call scenarios not covered by Secure UNIStim Graceful Failover

Although the Secure UNIStim Graceful Failover solves the IP Phone re-registration issue during SMC failover, it does not handle all call scenarios when device failure is encountered. The following are examples of possible failure scenarios.

Conferencing Call scenario

1. Phone A requests a conference.
2. The Signaling Server receives the request and forwards the request to the Conference Server.
3. The Signaling Server and Conference Server communicate through an existing TCP pipe, as shown in Figure 8.

Figure 8
MeetMe conferencing



4 The Conference Server grants the request, and the conference call is successful.

5 SMC1 fails and SMC2 becomes the new master.

6 Phone A attempts to make another conference call but the call fails.

7 Phone A must wait ten minutes before attempting the call again.

Root cause of failure

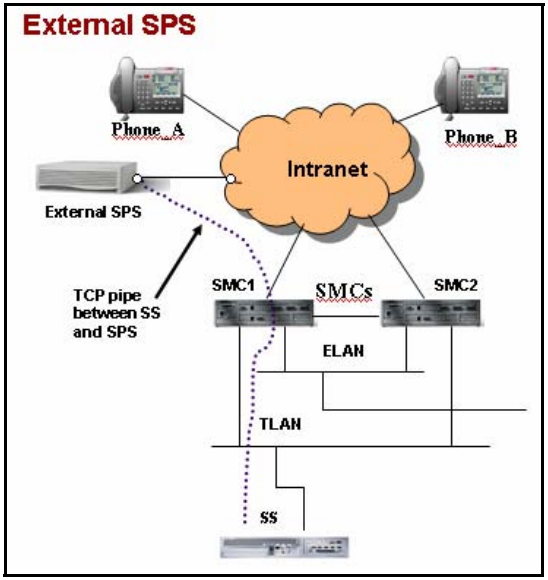
The TCP pipe connecting the Signaling Server and Conference Server is routed through SMC1. There is no corresponding pipe on SMC2. When SMC2 becomes the master, the SMC2 firewall drops all packets between the Signaling Server and the Conference Server. After ten minutes, the original TCP session times out. A new session is made through SMC2, after which conference calls can be made.

Calls through the external SIP Proxy Server scenario

1 Phone A dials an external number.

2 The Signaling Server consults the external SPS to resolve the number, as shown in Figure 9.

Figure 9
External SPS



3 The consultation is successful, and the call is made.

4 The call hangs up. SMC1 fails.

5 Phone A immediately dials another external number, but the call fails.

6 Phone A must wait ten minutes before attempting to dial another external number.

Root cause of failure

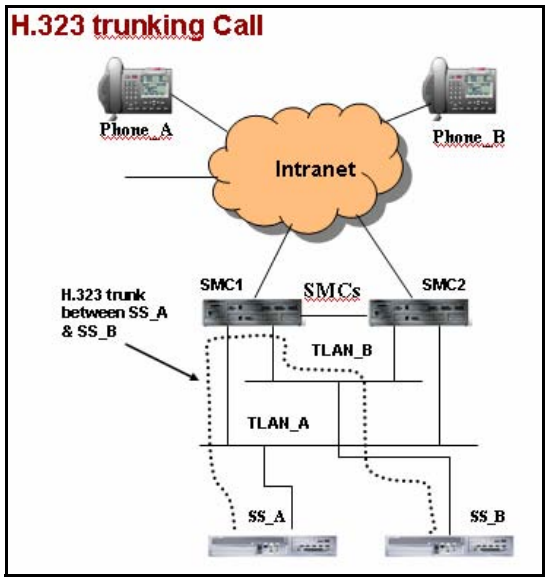
The TCP pipe between the Signaling Server and the SPS is not maintained on SMC2.

H.323 Trunking Call scenario

1 Phone A is registered through Signaling Server A Phone B is registered through Signaling Server B.

2 Phone A calls Phone B, and an H.323 trunk is established between Signaling Server A and Signaling ServerB, as shown in Figure 10.

Figure 10
H.323 Trunking Call



3 The call hangs up. SMC1 fails.

4 Phone A attempts to make the same call immediately, and the call fails.

Root cause of failure

The previous H.323 trunk (TCP) is still there through SMC1. The SMC2 firewall drops the TCP packets between Signaling Server A and Signaling Server B since there is no context.

Failure analysis

These scenarios have one thing in common; they all involve at least one TCP pipe through the active SMC. When the active SMC fails, since the same pipe is not maintained on the backup SMC, the SMC firewall cannot get the TCP packets through.

These issues can be resolved with the Port Bypass feature on SMC. With Port Bypass, the SMC firewall processing of packets is bypassed, so there is no need to maintain the duplicate pipe on the secondary SMC.

Port Bypass introduces risks to system security due to the open holes. As well, the user must know how to configure Port Bypass correctly in order for it to function properly.

For more information on Port Bypass, see “TCP Failover and Port Bypass” on page 45.

Geographic redundancy

Geographic redundancy is a CS 1000 failover architecture, consisting of a primary and secondary CS 1000. Each CS 1000 is identically configured and synchronized through the WAN.

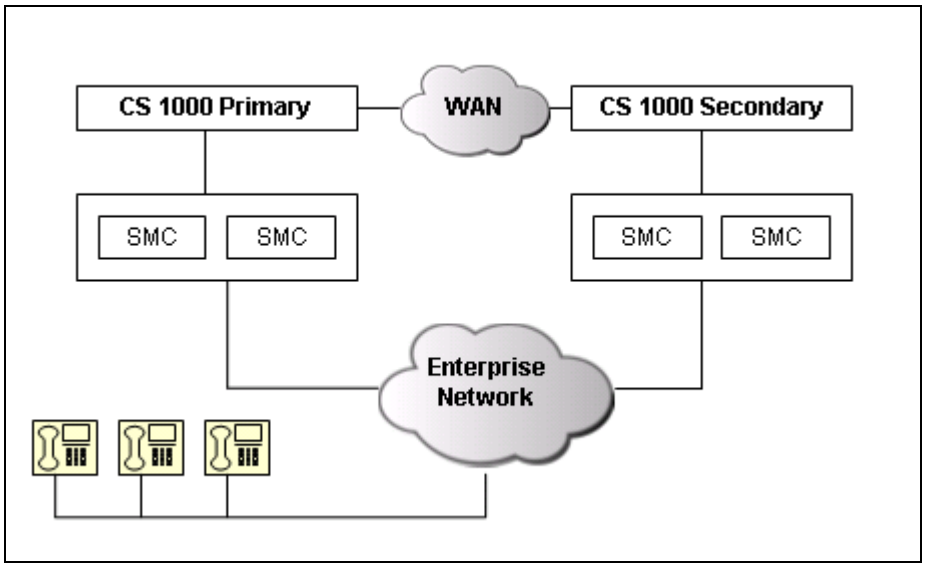
In geographic redundancy, an SMC installation must be present at each CS 1000 site so the traffic, after it fails over from one location to another, continues to be protected by an SMC.

Both SMC clusters must be managed independently for configuration changes and software updates.

Geographic redundancy

The general location of the SMCs in the geographically redundant installations is shown in Figure 11. Note that each site has a High Availability SMC setup, consisting of an active and a backup device. On a geographic failover from the primary CS 1000 to the secondary, the traffic is redirected to the second SMC cluster. The IP Phones re-establish a secure UNIStim connection with the SMC before access permission is granted to the CS 1000 Signaling Servers.

Figure 11
Geographic redundancy



Secure UNIStim keys

Because the IP Phones have limited space to store Secure UNIStim fingerprints, the private keys on the two SMC clusters must be defined appropriately.

If the IP Phones support two fingerprints, the two SMCs can have different private fingerprints; however, automatically generating two private fingerprints can be difficult. If the SMC initially sets the IP Phone fingerprints, the new fingerprint overwrites both fingerprint locations. A subsequent fingerprint update modifies only one of the fingerprints, thereby leaving two different fingerprints that can be specified uniquely for the primary and secondary devices.

Note: Nortel recommends that both SMC clusters share the same private key, and hence fingerprint, in a geographically redundant configuration.

Engineering impact and limitations

Buffering

Buffering and moving larger packets and small packet performance could be a limitation for high-end systems. Nortel estimates that the hardware provides at least 100 megabytes (MByte) throughput for 100 byte packets or 125 kilo packets per second (Kpps). This is sufficient to support more than 1000 concurrent calls, assuming 50 to 100 pps/call.

Security log rate limiting

In the following circumstances, the security and firewall logs can use many system resources and degrade performance:

- logging is turned on for a rule that processes many packets per second
- the SMC is installed in an environment where there is much additional traffic that is not handled by the current rules and logging is turned on for unavailable messages
- the SMC is under certain types of attacks
- a message is logged for every packet

These circumstances can degrade the performance of the SMC. Modifying logging configuration can help to overcome these issues. For more information, see “Logging” on page 213.

Port recommendations

Nortel recommends that port 1 be used for the management subnet, port 2 for the intranet subnet, and ports 3 through 6 for the secure multimedia zones.

Product compliance

For a complete list of supported products, Nortel recommends that you refer to the release notes post on the Nortel Web site.

For release notes, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

Hardware installation

Contents

This chapter contains information about the following topics:

Installation package contents

Table 2 lists the contents of the SMC 2450 installation package.

Table 2
Package contents

Item	Purpose
North American power cord	To meet North American power specifications. Not supplied if an alternate country cord is ordered.
European power cord	To meet European power specifications. Not supplied if an alternate country cord is ordered.

Table 2
Package contents

Item	Purpose
Console cable	To connect the SMC to a personal computer or local terminal
Bezel adapter kit with (2) brackets and (4) rubber feet	To install the SMC on a flat surface
Set of (4) mounting screws	To install the SMC in a rack
Secure Multimedia Controller: Implementation guide (553-3001-225)	SW/Doc kit

SMC physical features

The SMC front panel has buttons and indicators for normal operation. The front panel bezel is removable for access to the CD drive. The SMC rear panel has port and power supply access.

Front panel

Figure 12 shows the SMC front panel view. Table 3 describes front panel features.

Figure 12
Front panel view with bezel

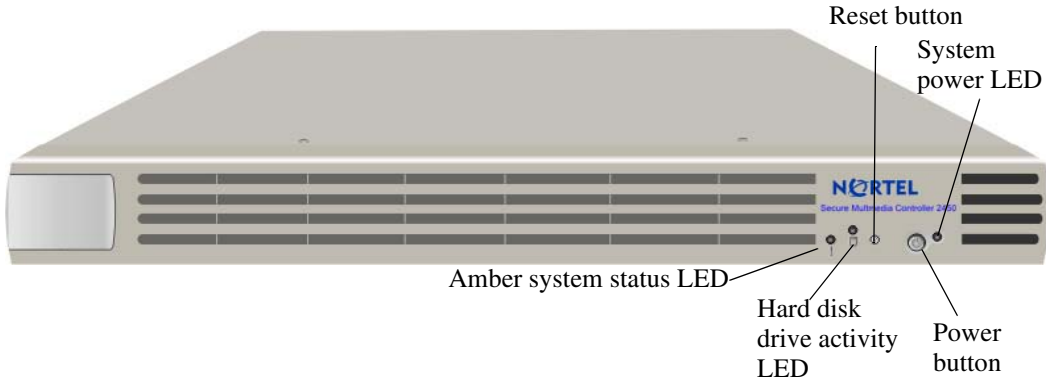


Table 3
Front panel features

Indicator or Button	Description
Amber system status LED	On when system needs attention due to power supply, fan, CPU, or device temperature problems
Hard disk drive activity LED	Blinks during hard disk drive activity
Reset button	Reboots the SMC
Power button	Turns on or off SMC power
System power LED	Shows green when power is on

Removing the front panel bezel

Remove the bezel for CD drive access. When you no longer require CD drive access, replace the bezel.

To remove the bezel, follow these steps:

1. On the left front of the unit, locate and open the bezel release flap (Figure 13).
2. Grasp the bezel and slide the bezel to the right until disengaged.

3 Remove the bezel from the faceplate.

End of Procedure

Figure 13
Bezel removal

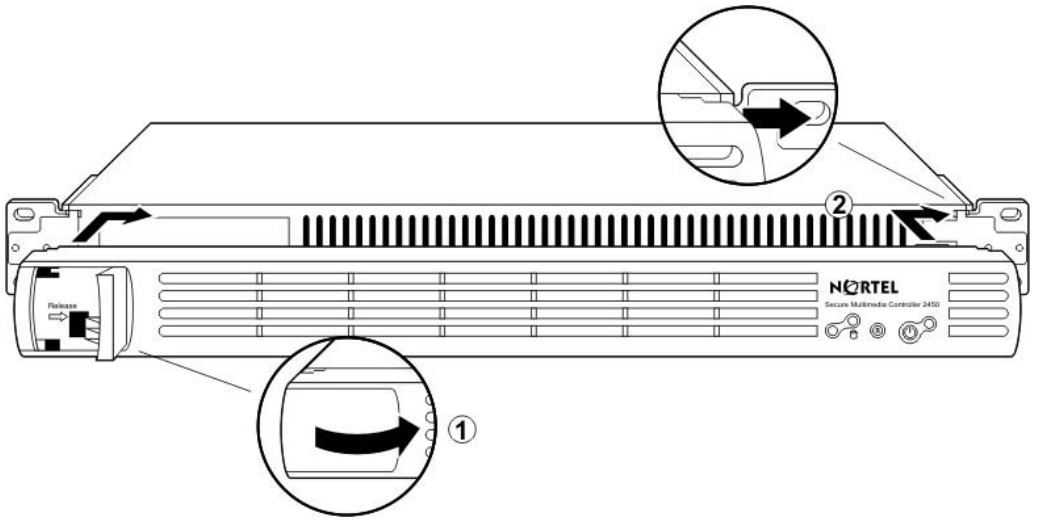
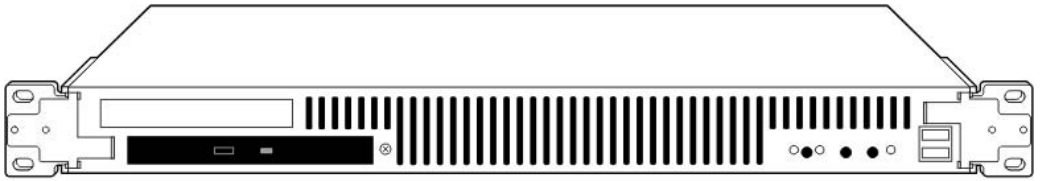


Figure 14 shows the front panel without the bezel.

Figure 14
Front panel view without bezel



Attaching the front panel bezel

Attach the bezel for normal operation.

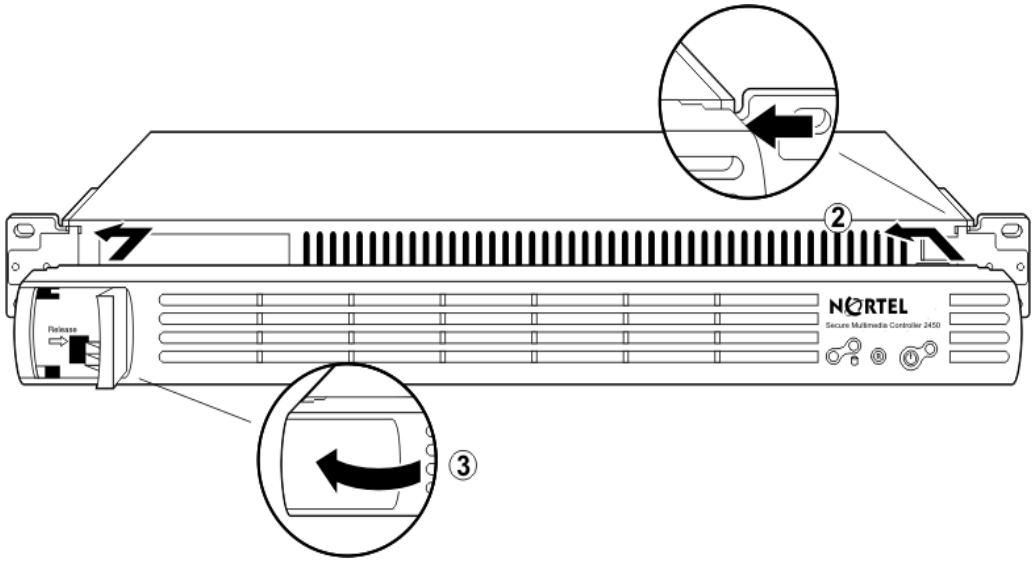
Procedure 1
Attaching the front panel bezel

To attach the bezel, follow these steps:

1. Align the bezel on the faceplate slightly to the right of the front panel.
2. With the release flap open, engage the bezel onto the track and slide it to the left until it locks into place (Figure 15).
3. Close the release flap.

End of Procedure

Figure 15
Bezel attachment



Rear panel

Figure 16 shows the SMC rear panel view. Table 4 describes rear panel features.

Figure 16
Rear panel view

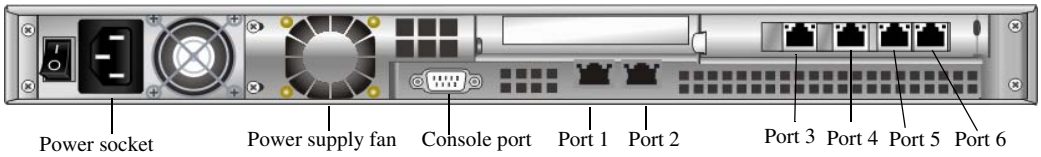


Table 4
Rear panel features

Item	Purpose
Power supply fan	Cools the power supply
AC power socket	Connects to the power source
Console port	Connects to the terminal or PC terminal emulator
LAN ports	Connect to the network

All ports are Gigabit 10/100/1000 LAN ports. Ports 1 and 2 are on-board ports. Ports 3 through 6 are NIC (Network Interface Controller) ports. Nortel recommends that port 1 be used for the management subnet, port 2 for the intranet subnet, and ports 3 through 6 for the secure multimedia zones. Status LEDs for each port are located above the port.

Table 5 explains LED status indicators for ports 1 and 2.

Table 5
Ports 1 and 2 LED status indicators

Port speed	Left LED (link)	Right LED (traffic)	Status
10 Mb/s	Off	Green/ flashing	Port operates at 10 Mb/s. Cable connection between the port and network device (switch, hub, or router) is working. When the right LED is flashing, the port is sending or receiving network data. The flash frequency varies with the amount of network traffic.
100 Mb/s	Yellow/flashing	Off	Port operates at 100 Mb/s. Cable connection between the port and network device is good. When the left LED is flashing, the port is sending or receiving network data.
1000 Mb/s	On or flashing	On or flashing	Port operates at 1000 Mb/s. Cable connection between the port and network device is good. When the LEDs are flashing, the port is sending or receiving network data.
All speeds	Off	Off	One or more of the above conditions is not met.

Table 6 explains LED status indicators for ports 3 through 4

Table 6
Ports 3 through 6 LED status indicators

Port speed	Left LED	Right LED	Status
10 Mb/s	Off	Green	Port operates at 10 Mb/s. Cable connection between the port and network device (switch, hub, or router) is good.
100 Mb/s	Green	Green	Port operates at 100 Mb/s. Cable connection between the port and network device is good.
1000 Mb/s	Red	Green	Port operates at 1000 Mb/s. Cable connection between the port and network device is good.
All speeds		Flashing	Port is sending or receiving network data. Flash frequency varies with the amount of network traffic.
All speeds	Off	Off	One or more of the above conditions is not met.

Installation

This section provides step-by-step instructions for physically installing the components of the SMC. It is assumed that the other components of the network, such as routers, servers, hubs, and so on, are physically installed.

Note 1: For the required software setup, see "Installation and configuration" on page 97.

Note 2: The instructions in this chapter are for installing a single unit. For the procedure to interconnect SMCs in an HA configuration, see "Installing the redundant SMC" on page 118.

Required equipment

You can rack-mount the SMC in a standard 19 inch (in.) rack, or install it on a shelf or other flat surface. You need the following tools and supplies to install the components:

- #2 Phillips screwdriver
- straight edge
- someone to hold the unit in place while you secure it in the rack

Safety precautions

Read all safety precautions before installing or servicing this device.

CAUTION — Service Interruption

This device is a Class A product. In a domestic environment, this device can cause radio interference, in which case the user may be required to take appropriate measures.

Ventilation safety

The ambient temperature of an operating SMC must not exceed 35ºC. When installing the device in a closed or multi-unit rack assembly, consider that the operating ambient temperature of the equipment can be higher than the

ambient temperature of the room. Take appropriate steps to ensure that the device does not overheat.

For proper air circulation, the vents on the front and back of the device must not be blocked or obstructed by cables, panels, rack frames, or other materials.

Electrical safety

DANGER OF ELECTRIC SHOCK

Use only power cords that have a grounding path. Without a proper ground, a person who touches the SMC is in danger of receiving an electrical shock. Lack of a grounding path to the SMC may result in excessive emissions.

To avoid the possibility of serious personal injury or damage to equipment due to electrical malfunction, follow these precautions.

- Circuits and wiring must support the rated power draw of the equipment.
- Total rack-power load is equal to a maximum of eighty percent of the branch circuit rating.
- Power cords are free of obstructions.
- Power cords at plugs, convenience receptacles, and points of exit from the SMC are carefully positioned.

Mechanical safety

CAUTION — Service Interruption

When mounting the SMC in a rack, *each* SMC must be secured to the rack with appropriate mounting brackets. Each bracket is designed to support the weight of one SMC.

For rack mounted installation, ensure that racks are stable and securely installed.

Installing the SMC in a rack

Install the SMC in a rack using the four supplied rack mount screws. For rack installation. Nortel ships the SMC with the mounting brackets attached to the front of the unit.

Procedure 2
Installing the SMC in a rack

Follow these steps to install the unit in a rack:

1. Identify a rack location and hole spacing alignment.
2. Separately supporting the full weight of the unit, use a #2 Phillips screwdriver to seat the four mounting screws through the front brackets and into the rack frame.

End of Procedure

Result: you can now connect the power supply. See "Connecting the power supply" on page 71.

Installing the SMC on a shelf or tabletop

Install the SMC on a flat surface using the supplied bezel adapter kit with 4 rubber feet.

Procedure 3
Installing the SMC on a shelf or tabletop

Follow these steps to install the unit on a flat surface:

1. Identify a stable shelf or tabletop location.
2. Using a #2 Phillips screwdriver, remove and replace the 2 rack mount brackets with the 2 bezel adapter kit brackets.
3. Remove the protective film from each of the supplied rubber feet and affix the feet to the four bottom corners of the unit.

End of Procedure

Result: you can now connect the power supply. See “Connecting the power supply” on page 71.

Supplying power to the SMC

Supply power after installing the unit in a rack or on a flat surface. Use of both the rear and front power switches is required for full SMC operation.

Power reliability

The SMC is a critical component in the enterprise communications system. The SMC does not support APC protocols for graceful shutdown in the event of power loss; therefore, you must ensure that the SMC power is supplied by a conditioned and backed-up source so that service is not interrupted in the event of a power loss or degradation.

Connecting the power supply

Connect the power supply using the power cord ordered for this location.

Procedure 4
Connecting the power supply

To connect the power supply, follow these steps:

1. Connect the power cord to the power receptacle on the unit's rear panel.
2. Plug the cord into a properly fused outlet.
3. Set the rear power switch to the "I" ON position.
4. Switch the power on by pressing the power button on the front panel. The system power LED turns green to indicate that power is supplied.

End of Procedure

IMPORTANT!

For normal use, switch the power on. Always disconnect the power before removing the unit from its installed location. Disconnect the power by setting the rear panel power switch to OFF.

Setting up terminal access to the SMC

The SMC has a console port for system diagnostics and configuration. This section explains how to connect a terminal to the console port to establish a first console connection.

For instructions on viewing and configuring system settings using either a console connection or network connection (via Telnet or SSH), see the "Installation and configuration" on page 97.

Terminal requirements

Before you establish a connection with a SMC, make sure you have the following required components:

- An ASCII terminal or a computer running ASCII terminal emulation software (standard terminal emulation type is VT100) with the parameters shown in Table 7.

Table 7
Console configuration parameters

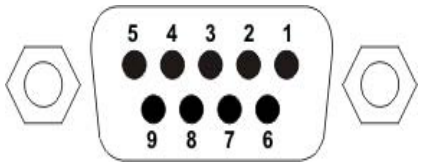
Parameter	Value
Baud Rate	9600
Data Bits	8
Parity	None
Stop Bits	1
Flow control	None

- A console cable, male to female, with DB-9 connectors and a straight cable as shipped with the SMC 2450.

Console connector and pin assignments

The console port on the unit is a DCE female DB-9 connector. Table 8 describes pin signal and I/O assignments for this connector.

Table 8
Pinouts for DB-9 console connector

DB-9 Console Port Connector	Pin	Signal	I/O	Description
	1	DCD	O	Data carrier detect
	2	RXD	O	Received data
	3	TXD	I	Transmitted data
	4	DTR	I	Data terminal ready
	5	GND	N/A	Signal ground
	6	DSR	O	Data set ready
	7	RTS	I	Request to send
	8	CTS	O	Clear to send
	9	RI	O	Ring indicator
	Shell	N/A	N/A	Chassis ground

Establishing a console connection

Establish a console connection by cabling the unit to a terminal or a computer running a terminal emulator session.The standard terminal emulation type is VT100.

Procedure 5
Establishing a console connection

To establish a console connection, follow these steps:

1. Using the supplied console cable, connect the terminal to the console port.
2. Power on the terminal and the SMC.

3 To initiate the system connection process, press <Enter> on the terminal.

4 At the login prompt, log on as user: **admin**.

5 At the password prompt, enter the administrator password. The default administrator password is **admin**.

WARNING

If you change the default password, Nortel strongly recommends that you record the new password. Passwords are not recoverable; if a password is lost, you must reinstall the SMC.

End of Procedure

Result: After password verification, the system displays the Setup menu.

Continue the set-up process using instructions for initial setup. See "Installation and configuration" on page 97.

Troubleshooting installation

Two situations require troubleshooting:

- The system does not power on correctly.
- The system powers on but shows no display text for initiating a session with the SMC.

No power

If the SMC does not power on with LED activation and fan operation as described, perform the following checks:

- Ensure that the power cord is connected to the SMC and connected to the AC power source.
- Make sure the power source provides enough voltage and current. For power supply specifications, see "Hardware and power supply specifications" on page 231.

- Ensure that the power switch on the rear of the system is turned on. Press the front panel power button.

If the system does not power on correctly after checking these items, contact Nortel Technical Support at www.nortel.com/support.

No display text

If the system powers on and no boot messages or console prompt appears, perform the following checks:

- Make sure the console cable is securely connected to the SMC and the terminal or PC that is running the terminal session.
- Make sure you connected the console cable supplied with the SMC system.

If the system display does not function after checking these items, contact Nortel Technical Support at www.nortel.com/support.

Firewall deployment

Contents

This chapter contains information about the following topics:

Introduction

This chapter provides information for both a stand alone and a HA configuration, although the diagrams show a HA system. See “High Availability (HA) configuration” on page 98 to review the configuration required to set up a High Availability cluster. Additional chapters in this document detail advanced SMC architectures such as geographic redundancy and campus redundancy.

Network placement

The SMC is a layer-3 device in the path of traffic between the insecure intranet and the Secure Multimedia Zones (SMZ), which is where the CS 1000 and MCS multimedia equipment resides. The SMC supports six

subnets: two mandatory subnets (management and intranet) and up to four optional subnets used for the SMZs.

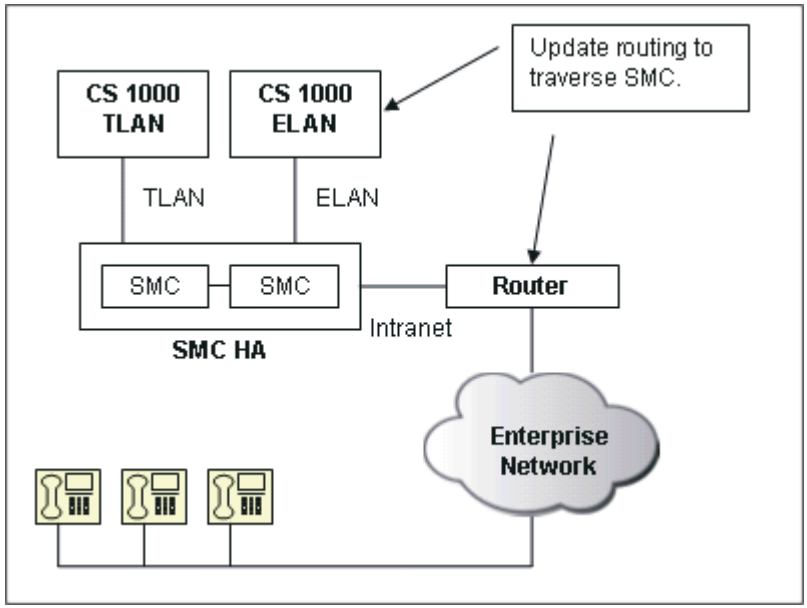
For more information about subnets, see "Overview of the deployment process" on page 17.

Routing updates

When you integrate an SMC into a network, you may need to update the routing tables on the devices on either side of the SMC so that traffic is directed through the SMC. The routing updates affect the VoIP equipment in the multimedia zones and the router that interfaces to the intranet.

Figure 17 on page 78 illustrates the devices that require routing updates.

Figure 17
Routing updates



Unhooking the firewall

Prior to placing the SMC into full service, disable (or unhook) the firewall and allow all traffic to flow through the SMC. Nortel recommends that the SMC be brought into service and utilized for a period of time in the unhooked state to ensure all network issues have been resolved.

IMPORTANT!

When the firewall is unhooked:

- SMC firewall protection is disabled
- Secure UNIStim capability is disabled
- Users may experience performance degradation when large number of media packets are traversing through the SMC

Procedure 6
Unhooking the firewall

1. Log on to the Web UI.

   Note: This procedure cannot be performed using the CLI.

2. Navigate to the **Multimedia Security > Security Settings > Status** page.
3. Unhook the firewall.
4. In a High Availability configuration, select the second SMC device from the IP address drop-down list and unhook its firewall.

End of Procedure

Validating unhook

To validate that the firewalls are unhooked, view the firewall status on the initial System page of the Web UI.

Note: You can add and update firewall rules while the firewall is unhooked; however, the rules do not go into effect until the firewall is reactivated (hooked).

IMPORTANT!

When the firewall is unhooked, all traffic flows through the SMC unchecked or rate limited. Unhooking the firewall is recommended only for initial installation and debugging purposes.

IMPORTANT!

If the firewall is hooked or unhooked while UNIStim security is enabled and the IP Phones are communicating through a proxied server, current UNIStim sessions are disrupted. UNIStim communication re-establishes and all existing calls drop. Insecure sessions—sessions that are not currently running through the Secure UNIStim proxy—are not affected.

Network integration

After the firewall is unhooked, you can add the SMC to the network and update the routing on the connected devices. Current services are not disrupted after configuration is complete. Packets are routed to and from the SMZs and the presence of the SMC does not affect current network functionality.

Hooking the firewall

After you verify the SMC placement, you can turn the firewall on. If the firewall rules are properly configured, the traffic and services continue through the SMC as they did prior to SMC integration.

Procedure 7
Hooking the firewall

Nortel strongly recommends that you hook the firewall during a maintenance window.

1 Log on to the Web UI.

Note: This procedure cannot be performed using the CLI.

2 Navigate to the **Multimedia Security > Security Settings > Status** page.

3 Hook the firewall.

4 In a High Availability configuration, select the second SMC device from the IP address drop-down list and hook its firewall.

End of Procedure

IMPORTANT!

The SMC is a stateful firewall; therefore, it requires Transmission Communication Protocol (TCP) connections to establish a session before the traffic is allowed. This means that:

- Current TCP connections flowing through the SMC, such as CallPilot or OTM sessions, are terminated and required to recreate a session even if there is an applicable rule for the connection.
- Current Telnet and Secure Shell (SSH) connections are terminated and required to re-establish communication.
- User Datagram Protocol (UDP) sessions may not be affected. Current UNIStim calls, including media, continue to flow as previously because they are based on UDP.

IMPORTANT!

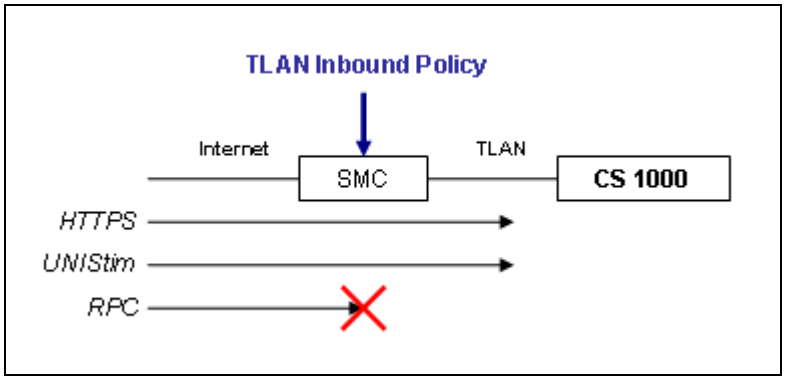
H.225 connections used in H.323 communication, such as IP Peer Trunks, are based on TCP and have a timeout value of 15 minutes when interrupted. Trunk calls can be blocked. The SMC supports a port bypass for the H.225 protocol, which runs on port 1720. With a bypass, the SMC does not firewall the traffic; therefore, the traffic is not interrupted when the firewall is hooked or during failover. The H.225 port bypass is added automatically when you generate TLAN rules at initial configuration.

Troubleshooting firewall policies

After you hook the firewall, any problems, such as services no longer working, are generally caused by the firewall blocking traffic that should be allowed through. These problems are likely due to missing firewall policies. You can troubleshoot the firewall policies by first determining what traffic is denied and then adding an appropriate policy for the relevant SMZ.

Figure 18 shows HTTPS and UNIStim traffic flowing correctly through the SMC. Note that the RPC traffic is blocked by the firewall because a rule for the RPC protocol is not included in the default TLAN rule set.

Figure 18
HTTPS and UNIStim traffic flow



Use the following methods to troubleshoot firewall problems:

Allowing ping

If end-to-end connectivity between the client and the server is in question, it is helpful to allow ping to pass through the SMC so the client can validate that packets are correctly routed to and from the server.

By default, ping is not allowed through the firewall for security reasons. To allow ICMP packets to flow through the SMC and thereby enable ping, add an inbound rule to the appropriate Security Zone and choose ICMP as a custom service. The Security Zone should be the one in which the accessed server is located.

Procedure 8
Allowing ping

In this procedure, the TLAN security zone is used as an example.

1. Log on to the Web UI.
2. Navigate to **Multimedia Security > Security Zones > tlan > Inbound Rules.**
3. Click **Add**.
4. Select **Custom** as the service.
5. Select **ICMP** as the protocol.
6. Select the appropriate Source and Destination for the client and server.
7. Set Action to **allow**.
8. Click **Update**.
9. The rule will be added to the end of the current list.
10. Click **Apply** to save the current configuration.

End of Procedure

Result: You can ping the server through the SMC. If you allowed pinging, and the SMC is still blocking the traffic, verify connectivity between the client and the SMC, and between the SMC and the server. Nortel recommends that you disable the ICMP rule when not in use.

Firewall logs

Using the Web UI, you can view firewall logs by stepping through the logs in chronological order or view a specific log by specifying an appropriate search string, such as the IP address of the problem machine. Viewing the firewall logs is the best method to troubleshoot packets that are not traversing the SMC.

IMPORTANT!

When the SMC starts up for the first time, firewall logging is limited to prevent the generation of too many log messages. For troubleshooting purposes, increase the number logging messages and then turn them off when troubleshooting is completed. The two most useful messages not sent by default are:

- log messages associated with a specific rule
- log messages associated with Unavailable policies, which are logged when a packet does not map to any policy in the rule list and is dropped.

Procedure 9
Viewing firewall logs

1. Log on to the Web UI.
2. Navigate to **Logs > Security Log**.
3. Click **Search**.

The latest firewall log messages are displayed.

4. Enter the IP address of the client or server of the problem machine.
5. Click **Search**.

End of Procedure

Result: All logs for that machine are now listed.

Unavailable policy logging

When a packet hits the firewall and there is not a rule to match it, it is silently dropped without logging a message. These dropped packets may be from services that are failing when the SMC is placed within the path of the traffic; therefore, logging these messages (called unavailable policies) is critical to determining which additional rules are required for a particular installation.

Procedure 10
Enabling unavailable policy logging

1. Log on to the Web UI.
2. Navigate to **Multimedia Security > Security Settings > Log > Messages**.
3. Enable **Unavailable Policies**.
4. Click **Apply**.

End of Procedure

Result: The firewall logs now list additional packets that were dropped. These packets can be correlated to the IP addresses of the client to determine which ones are being dropped.

An example of an unavailable policy entry:

```
Mar 1 13:01:37 127.0.0.1 id=firewall time="2006-03-01
13:01:37" fw=a10-10-10-10 pri=4 proto=6(tcp)
src=2.2.2.100 : 32802 dst=3.3.3.200 : 22 mid=2076 mtp=10
msg="Access Policy not found, dropping packet from ext n/
w" agent=Firewall
```

Mapping rule IDs in the firewall log

Log messages are assigned a rule ID, which represents the dynamic identifier of this rule entry within the running firewall. You can use rule IDs to determine the exact rule that mapped the dropped packet.

IMPORTANT!

To generate log messages for specific firewall rules, you must enable logging for each rule and Allow/Deny log messages must be enabled in the **Multimedia Security > Security Settings > Log > Messages** page.

Rule IDs are not assigned to log entries for unavailable policies, because unavailable policies do not map to a particular rule.

The rule ID is different than the numerical identifier assigned to a rule during firewall configuration. The numerical identifier is used only for ordering the rules.

IMPORTANT!

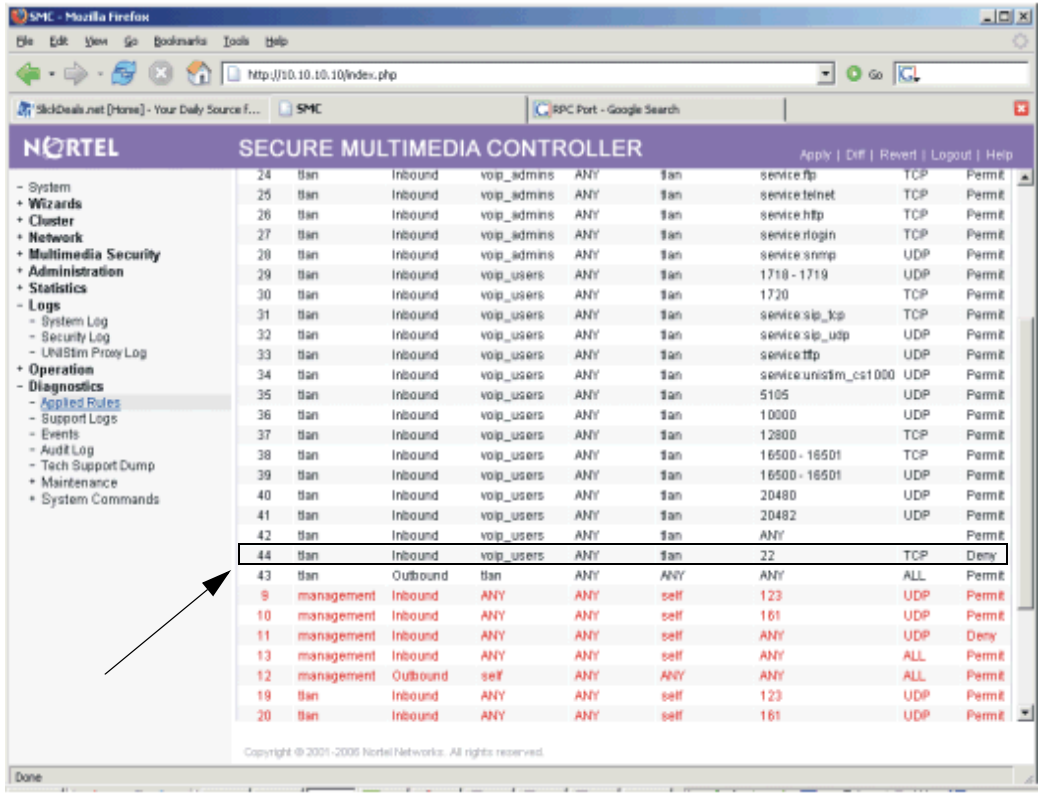
Because the entries in the Applied Rules list are dynamic, their rule IDs may change when the SMC is restarted; therefore, it is important to map the entries in the firewall log with those in the running SMC.

A sample firewall message generated when a Deny rule is hit by a packet:

```
Mar 1 13:21:14 127.0.0.1 id=firewall time="2006-03-01
13:21:14" fw=a10-10-10-10 pri=1 proto=6(tcp)
src=2.2.2.100 : 32808 dst=3.3.3.200 : 22 mid=2077 mtp=7
msg="Deny access policy matched, dropping packet from ext
n/w" ruleid=44 agent=Firewall
```

Note that logging was previously enabled for this rule within the configuration. The rule ID is 44. Figure 19 on page 87 shows that rule 44 maps to TCP protocol 22 (SSH).

Figure 19
Rule 44 mapping to TCP protocol 22 (SSH)



Procedure 11
Viewing applied rules

1 Log on to the Web UI.

2 Navigate to **Diagnostics > Applied Rules**.

Note: The Applied Rules page defines all currently applied rules on the firewall, not just the rules specified in the configuration inbound/outbound lists. Additional rules are listed for secure UNIStim server traffic and self traffic, which is traffic to and from the SMC device. The basic firewall rules do not map to the configuration rules perfectly (for example, duplicate rules are removed).

3 Search for the appropriate rule ID.

4 Determine the details of the rule.

End of Procedure

Downloadable firewall rules from WebUI

Log messages reference the ruleids defined by the firewall. To parse log messages the user must map the ruleids to the rules being applied on the firewall.

To view and download the rules being applied on the firewall, navigate to the **Diagnostics > Applied Rules** page of the Web UI. From this page of the Web UI, the firewall rules can be searched by ruleid and selected zone. Color codes are used on this page to distinguish user defined rules from auto-generated rules.

System log

To determine why particular traffic is not traversing an SMC, you can explore the current system logs to make sure there are no system-level failures affecting connectivity.

Procedure 12
Viewing the system log

1 Log on to the Web UI.

2 Navigate to **Logs > System Log**.

3 Click **Search**.

4 Click **Next Page** to step through the log messages.

End of Procedure

System and host status

You can view the system status for each SMC in the cluster.

Procedure 13
Viewing system and host status

1. Log on to the Web UI.
2. Navigate to the **Administration > Monitor > System** page to see the status of the Secure UNIStim security, current alarms and the overall status of each host in the cluster.
3. Navigate to **Administration > Monitor > SMC Hosts** to view host and application status.

End of Procedure

Advanced networking

To view the UNIX-based IP configuration and ARP tables, navigate to the **Diagnostics > System Commands** page.

Custom firewall rules

If you determine that specific traffic is dropped by the SMC because an appropriate firewall rule does not exist, you can add a custom inbound rule to allow this traffic through. The rule should map the source and destination networks for the traffic, the protocol (either TCP, UDP, SVP, or ICMP), and the port (if not ICMP or SVP).

Procedure 14
Create a customer inbound rule

1. Log on to the Web UI.
2. Navigate to **Multimedia Security > Security Zones > tlan > Inbound Rules**.
3. Click **Add**.
4. Designate Service as **Custom** with the appropriate protocol.
5. Select the **Source** and **Destination** for the client and server networks.
6. Set Action to **allow**.
7. Click **Update**.

8 Click **Apply** to save the current configuration.

End of Procedure

Result: The rule is added to the end of the current list. It is usually helpful to turn on logging for new rules, at least until you are sure they are working appropriately.

IMPORTANT!

Firewall rules are evaluated in top-down fashion. The rules with lower IDs have precedence over rules with higher IDs. You can reorder rules to customize the order in which they are evaluated.

IPsec traffic

To specify IPsec ESP and IPsec AH as custom protocols while creating firewall rules, navigate to the **Multimedia Security > Security Zones > mcslan > Inbound Rules** page of the Web UI.

Extensible firewall rule templates

The SMC has a set of default XML files (rule templates) that it uses in rule generation when firewall inbound/outbound policies are created for a Security Zone.

The user can

- view and download the rule templates.
- edit, extend and enhance the rule templates.

To use this functionality navigate to the **Multimedia Security > Security Settings > Automatic Rules** section of the Web UI. From this section of the Web UI the user can

- list all the current Automatic Rule XML files on the system

- View, Download and Delete the XML files
- view and download the XML Schema used in creating the XML files used in Automatic Rule Generation.

Example usage of extensible firewall rule templates

See Procedure 15 on page 91 for an example usage of the extensible firewall rule templates. To incorporate changes from MCS 3.x to MCS 4.x, in Procedure 15 the firewall rules are modified for the MCS LAN to add MCP ports 12120 and 12121, and to add Provision Manager port 8443.

Procedure 15
Add new port information for MCP and Provision Manager to MCS LAN firewall rules

1. Log on to the Web UI.
2. Navigate to **Multimedia Security** > **Security Settings** > **Automatic Rules** > **XML Files**.
3. Download the SMC rules file for MCS LAN.
4. Edit the saved file and add the following text within the <inbound></inbound> tag:

```
<rule>
    <comment>MCP</comment>
    <source>user</source>
    <destination>zone</destination>
    <cservice>
      <minport>12120</minport>
      <maxport>12121</maxport>
      <protocol>tcp</protocol>
    </cservice>
    <action>allow</action>
  </rule>
  <rule>
```

```
<comment>Provision Manager</comment>
<source>user</source>
<destination>zone</destination>
<cservice>
  <minport>8443</minport>
  <maxport>8443</maxport>
  <protocol>tcp</protocol>
</cservice>
<action>allow</action>
</rule>
```

5 Import the updated file from the **Multimedia Security** > **Security Settings** > **Automatic Rules** > **XML Files** Web UI page.

Note: The update will be applied and the changes will be reflected automatically in the SMC upon successful import of the updated XML file.

End of Procedure

Configuring CallPilot desktop messaging

CallPilot Desktop Messaging requires ICMP packets to be exchanged between the Desktop Messaging Client and the CallPilot Server, which is normally present in the Server LAN. SMC rule auto-generation does not include an explicit ICMP rule; you must add ICMP support manually using the CallPilot Desktop Messaging Wizard.

Using the CallPilot Desktop Messaging Wizard, you can specify an ICMP rule to allow the Desktop Messaging Client to communicate with the CallPilot Server. Flow control is used to limit the number of ICMP packets transmitted per second.

Before starting, gather the following information:

- Approximate number of Desktop Messaging Clients
- IP address of the CallPilot Server(s)

Procedure 16
Configuring CallPilot Desktop Messaging

1. Log on to the Web UI.
2. Navigate to **Wizards > Firewall > CallPilot Desktop Messaging**.
3. Specify a client network accessing the CallPilot servers.

   In the default configuration, the client network is the voip_users network.
4. Specify the security zone in which the CallPilot servers exist.

   If servers are present in more than one security zone, then the Wizard must be run for each zone.
5. Click **Next**.
6. Specify an ICMP rate limit for this rule.

   CallPilot Desktop Messaging requires ICMP to flow between clients and servers. Since this potentially could lead to ICMP flooding, the rule requires a rate-limiting flow. The packet limit can be approximated by estimating approximately 5 packets per second per CallPilot Desktop Messaging Client divided by 10, to represent 10% of clients connecting simultaneously. You can either use a pre-existing flow on this page, or have one created for you.
7. Click **Next**.
8. Specify the IP addresses of the CallPilot Servers.

   At this page, you can add servers and tie them to a network.
9. Click **Finish**.

10 Click **Apply**.

End of Procedure

Result: The CallPilot Desktop Messaging Wizard creates a new network for the Desktop Messaging Servers and adds an appropriate rule to the designated Security Zone. If a new flow was created, it would be added to the list of flows as well. Note that the allow rule will be appended to the end of the current Inbound Rule list for the Security Zone. If you have added an explicit deny rule for this traffic prior to this rule, then the rules position may need to be altered before the ICMP traffic is allowed.

Configuring Symposium multicast

Symposium uses multicast to send Real Time Data (RTD) to the Symposium Web Client (SWC) Server and the SWC Server uses multicast to send RTD to Web Clients. The Web Clients use HTTP (Port 80) or HTTPS (Port 443) to connect to the SWC Server. These components of Symposium can be in the same network or across multiple networks. If these components are across multiple networks, all the routers in between these individual components need to support multicast routing. The SMC is one of the routers that can be deployed in between these Symposium components.

The ports and multicast addresses used by symposium components are:

- A configurable multicast address on SWC Servers (SWC Server to Web Clients for RTD)
- Port numbers 7020 to 7130 in increments of 10
- A configurable multicast address on Symposium Server (Symposium Server to SWC Server for RTD)
- Port numbers 6020 to 6130 in increments of 10(Symposium Server to SWC Server for RTD)

Note 1: If the deployment has a single Symposium Server and single SWC Server, they are generally collocated. Some deployments have multiple Symposium Servers use a single SWC Server.

Note 2: Optionally, Symposium components can use unicast in place of multicast for Real Time Data.

As SMC does not support multicast, SMC can be configured to bridge specific multicast traffic. The support for bridging is limited to only multicast packets. Wizards are provided to help configure the SMC to support the Symposium components that use multicast for RTD.

Procedure 17
Configuring Symposium multicast

1. Log on the Web UI.
2. Navigate to **Wizards > Symposium Multicast**.
3. Select one of the following options:
   - Communication between the SWC Server and Web Client
   - Communication between the Symposium Server to the SWC Server
4. Click **Next**.
5. Specify the source and destination security zones.

   The source security zone is where the multicast traffic originates, such as the SWC Server or the Symposium Server. The multicast IP address is also defined on this page.
6. Select **Finish**.
7. Click **Apply**.

End of Procedure

Result: Multicast bypass is enabled and an entry is made into the Multicast Bypass List located in the Web UI at: Multimedia Security > Multicast Bypass.

voip_users and voip_admins

voip_users and *voip_admins* are default networks added when the SMC is initially configured. These default networks are placeholder networks used in rule creation. The networks are fully customizable and have no relevance other than as placeholders.

voip_users

The voip_users network refers to user-level access; that is, access by IP Phones and other devices that use the multimedia services of the CS 1000 or MCS installations. By default, this network maps to all IP addresses. You can either constrain this definition to suit the internal network or redefine it as needed.

voip_admins

The voip_admins network refers to management-level access by subnets/IP addresses that can launch management applications on the VoIP/Multimedia equipment. By default, the voip_admins network defines no subnets and provides no access to these interfaces. You must update this network with specific management IP addresses or subnets before any auto-generated rules containing the network will be accessible.

Installation and configuration

Contents

This chapter contains information about the following topics:

SMC configurations

The SMC supports two types of configurations:

- Stand-alone
- High Availability (HA)

Stand-alone configuration

The stand-alone configuration contains a management network, intranet network, and one or more security zones. Each of the Secure Multimedia Zone (SMZ) networks requires a unique port on the SMC device and an IP address.

The management network needs two IP addresses in the stand-alone configuration. The first address is the host IP address, which is the IP address for the SMC. The second IP address is the cluster Management IP (MIP)

address. The host IP address and the cluster MIP address must reside in the same subnet.

IMPORTANT!

In a stand-alone configuration, the equipment residing on the SMZs uses the SMC Interface IP addresses as their gateway address. For example, a CS 1000 Signaling Server TLAN Gateway address is the SMC TLAN IP address

High Availability (HA) configuration

In the HA configuration, each SMZ requires three IP addresses: one IP address for each physical SMC interface and a Virtual Router Redundancy Protocol (VRRP) address. The VRRP address is hosted by the VRRP master and floats to the backup if the master fails. For more information about VRRP, see “VRRP overview” on page 179.

IMPORTANT!

In a High Availability configuration, the equipment residing on the SMZs uses the SMC Virtual IP addresses as their gateway address.

When upgrading from a stand-along SMC to a High Availability SMC installation, review carefully the IP addressing scheme so that the equipment in the SMZs do not need the gateway addresses changed.

For example, when upgrading from stand-alone to a High Availability configuration, change the IP addressing so the existing SMC interface IP addresses are used as the Virtual IP addresses when the HA config is implemented.

SMC network engineering worksheets

Table 9 and Table 10 on page 100 provides SMC network engineering worksheets for configuring the first SMC (or a stand-alone SMC) and the second SMC in a HA configuration. You can print these pages and use them to plan the IP addressing for the SMC configuration.

Table 9
SMC network engineering worksheet for first/stand-alone SMC

First / Stand-alone SMC Configuration					High Availability VRRP	
SMC Port	**Zone**	**IP Address**	**Mask**	**Gateway**	**Virtual IP**	**Virtual Router ID**
1	Management			n/a		
MIP address	Management		same as above	n/a	n/a	n/a
2	Intranet	See note		See note	See note	
3				n/a		
4				n/a		
5				n/a		
6				n/a		

Note: A static route may be required on the gateway router so packets from the Intranet (IP clients and Administrators) are routed to the SMC, which routes to the correct SMZ. In a stand-alone configuration, the static route points to the Intranet IP address. In a High Availability configuration, the static route points to the Intranet Virtual IP address.

Table 10
SMC network engineering worksheet for second SMC in a HA configuration

SMC Port	Zone	IP Address	Mask	Gateway	Virtual IP	Virtual Router ID
1	Management			same as first SMC	same as first SMC	
MIP address	Management	same as first SMC	same as above	same as first SMC	n/a	n/a
2	Intranet			same as first SMC	same as first SMC	
3				same as first SMC	same as first SMC	
4				same as first SMC	same as first SMC	
5				same as first SMC	same as first SMC	
6				same as first SMC	same as first SMC	

Table 11 provides a worksheet to identify other important IP addresses.

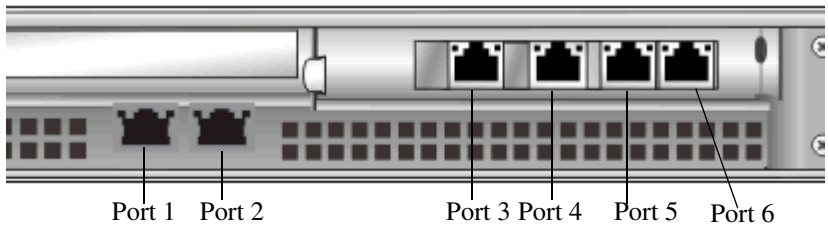
Table 11
Other important addresses and networks

Item	IP Address	Mask	Notes
SMC Admin PC/Subnet			Used in SMC Access List
CS 1000 Node IP		n/a	Unistim Clients
MCS-5100 IPCM		n/a	MCS-5100 Unistim clients
MCS-5100 App Server		n/a	MCS-5100 Soft Clients
SNMP Server		n/a	System Monitoring
SYSLOG Server		n/a	System Monitoring
FTP Server		n/a	Backup and Upgrade procedures
TFTP Server		n/a	Backup and Upgrade procedures
RADIUS Server		n/a	SMC Admin access authorization

Port mappings

Ports are located on the back of the SMC and have the numbering scheme shown in Figure 20.

Figure 20
SMC port mappings



Port recommendations

Nortel recommends that port 1 be used for the management subnet, port 2 for the intranet subnet, and ports 3 through 6 for the secure multimedia zones.

Configuring the initial SMC

To configure the initial SMC, you must use the Command Line Interface (CLI). The CLI is a text-based administrative and configuration tool, which is accessed using a basic terminal. After initial configuration, you can use either the Web User Interface (UI) or the CLI for administration and maintenance tasks; however, the Web UI is the preferred tool.

For more information about the administrative tools, see "The Command Line Interface (CLI)" on page 187 or "Web User Interface (UI)" on page 201.

IMPORTANT!

Note the following CLI conventions:

- The CLI is case-sensitive; therefore, type the commands as capitalized in this document.
- You can accept the default value in a command by pressing <Enter> on the keyboard.
- Use the backspace key to correct any errors you make before pressing <Enter> to execute a command.

Procedure 18
Configuring the initial SMC

Use this procedure to configure a stand-alone SMC or the first SMC in a High Availability configuration.

1 Disconnect the ethernet cable on all SMC ports except the management port.

2 Apply power to the SMC.

The SMC boots from the factory-installed software. The boot process takes approximately 5 minutes.

3 Connect the console cable to the SMC.

Connect the console cable from the serial port on the SMC to the serial port of a computer that runs terminal emulation software. Nortel recommends that you use VT100 for emulation and 9600-8-N-1 for the communication port speed on the terminal connection.

4 Start a console terminal.

5 Press <Enter> on the console terminal to establish the connection.

The SMC login prompt appears.

6 Enter **admin** for the default login name.

7 Enter **admin** for the default password.

The Setup prompt (>> Setup#) is displayed. If the Main prompt (>> main#) appears, the SMC is already configured. If you want to reset the SMC to factory defaults, see “SMC software upgrades” on page 168.

8 At the Setup prompt, enter **new** to set up a new configuration.

IMPORTANT!

If you make an error after step 8 and need to restart the procedure, press Ctrl + C. The CLI redisplays the Setup prompt and you can begin again step 8.

9 Initialize the management subnet.

a. Enter the port number for the management subnet.

b. Enter the IP address for this port.

c. Enter the network mask for the entire management subnet.

d. Enter the cluster Management IP (MIP) address information.

The cluster MIP address must reside in the same subnet as the IP address specified in step b.

Note: This is the IP address used to perform browser-based administration from the management subnet.

10 To configure the Web UI, choose one of the following:

a. Enter **yes** to enable Web administration on the management subnet.

b. Enter **no** to indicate you do not want to enable Web administration.

11 Initialize the intranet subnet.

a. Enter the port number for the intranet subnet.

b. Enter the IP address for the intranet subnet.

c. Enter the network mask.

d. Enter the gateway IP address.

12 Configure the cluster settings.

a. Set the time zone.

i. Select your continent or ocean.

ii. Select your country.

iii. Select your region.

b. To set the current date, choose one of the following:

— Enter the current date.

— Press <Enter> to accept the default.

c. To set the current time, choose one of the following:

— Enter the current time.

— Press **yes** to generate a new Secure Shell (SSH) host key.

Note: Nortel recommends that you generate a new SSH key to maintain a high level of security when connecting to the SMC using an SSH client. For more information about SSH, see “Using Secure Shell (SSH)” on page 189.

d. Enter a password for the administrator.

Note: You can optionally enter a new password for the admin user or you can enter and keep the default password if desired, and then change the password when the SMC is operating as desired.

e. Reenter the password.

WARNING

When you change the default password, Nortel strongly recommends that you record the new password. Passwords are not recoverable; if a password is lost, you must reinstall the SMC.

13 Enter **yes** to run the quick setup wizard.

The quick setup wizard creates the ELAN subnet, TLAN subnet, and other networks, and adds the baseline rules. Each network is defined by a port, IP address, and subnet.

14 Choose one of the following:

- Enter **yes** to indicate you have a CS 1000 setup.
- Enter **no** to indicate you do not have a CS 1000 setup.

If you entered **no**, go to step 18.

15 Configure the CS 1000 ELAN subnet.

a. Enter **yes** to configure the ELAN subnet.

b. Enter the port number for the ELAN subnet.

c. Enter the ELAN subnet IP address.

d. Enter the ELAN subnet netmask.

16 Configure the CS 1000 TLAN subnet.

a. Enter **yes** to configure the TLAN subnet.

b. Enter the port number for the TLAN subnet.

c. Enter the TLAN subnet IP address.

d. Enter the TLAN subnet netmask.

17 Configure the CS 1000 Server LAN subnet.

a. Enter **yes** to configure the Server LAN subnet.

b. Enter the port number for the Server LAN subnet.

c. Enter the Server LAN subnet IP address.

d. Enter the Server LAN subnet netmask.

18 Choose one of the following:

- Enter **yes** to indicate you have an MCS setup.
  i. Enter the port number for the intranet subnet.
  ii. Enter the IP address for the intranet subnet.

iii. Enter the network mask.

iv. Enter the gateway IP address.

- Enter **no** to indicate you do not have an MCS setup.

CS 1000 Result: The system initializes and rules generate for the ELAN subnet, TLAN subnet, and Server LAN subnet. The system logs you out and you must log on again to continue management on the SMC.

MCS Result: The MCS filters are configured. The system logs you out and you must log on again to continue management on the SMC.

End of Procedure

Accessing the SMC through the Web UI

Allowing remote Intranet access

If you enabled Web administration in step 10 of Procedure 18, the access list is updated automatically for Web browsers with IP addresses on the management subnet. If you chose not to enable Web administration, you must allow an Intranet client workstation remote access to the SMC.

In Procedure 19, you add the IP address of an Intranet client workstation for remote management access such as Telnet, Web User Interface (UI), or SSH. Entering a 32-bit mask (255.255.255.255) limits access to only that particular IP address.

Procedure 19
Allow remote Intranet access

1 If you are not already logged on to the SMC, perform the following steps:

a. Press <Enter> on the console terminal to establish the connection.

The SMC login prompt appears.

b. Enter the admin login name.

c. Enter the admin password.

The Main prompt (>> main#) is displayed.

2 Enter **/cfg/net/if intranet/mgmt**

3 Enter **`y`** to allow Web UI administration through the intranet.

4 Enter **`/cfg/sys/acc/add`**

5 Enter the network IP address of client workstation or the client subnet that you want to have Web UI administration access to the SMC.

Note: If you specify a single IP address that is currently in use on a PC, the IP address may change on the PC due to DHCP usage.

6 Enter the network mask.

Note: A mask of 255.255.255.255 will allow only the single IP address identified in step 5 to access the SMC system.

The Access list prompt is (`accesslist#`) is displayed.

7 Enter **`apply`** to apply the configuration changes.

8 (Optional) Repeat steps 4 through 7 to add more workstations.

End of Procedure

Result: Using a PC with the IP address identified in step 5 or address on the subnet, you can use a web browser to reach the SMC. For example, if the SMC intranet interface address was 10.1.1.2, you would browse to http://10.1.1.2. On a HA system, browse to the VRRP address shared on the intranet interfaces.

Enabling secure HTTP

Procedure 20
Enabling the Web UI

You can enable the Web UI for HTTP and/or HTTPS access. By default, the Web UI is enabled for HTTP access and disabled for HTTPS access.

Note: HTTP is not a secure protocol. All data (including passwords) between an HTTP client and the SMC is not encrypted and is subject only to weak authentication. If secure remote access is required, use HTTPS.

1 Access the CLI. See “Accessing the CLI” on page 188.

2 Choose one of the following:

- To enable HTTP access, enter
  >> # /cfg/sys/adm/web/http/ena.
- To enable HTTPS access using SSL, enter
  >> # /cfg/sys/adm/web/ssl/ena.

3 Generate a temporary certificate (if using HTTPS).

An SSL server certificate is required for HTTPS access to the Web UI. The SMC can generate a temporary, self-signed certificate.

a. Enter **>> SSL configuration# certs/serv/gen <Name> <Country code> <Key size>**.

where Name is the common name that appears on the certificate, Country code is a two-letter code (US for the United States of America, CA for Canada, JP for Japan, and so on), and Key size is 512, 1024, or 2048 bits.

For a list of country codes, refer to the International Standards Organization (ISO) website for the ISO 3166 standard for two-letter country codes.

For example:

>> SSL configuration# certs/serv/gen Nortel US 1024

b. Enter **Y** to verify that you want to generate a self-signed certificate with the generated key.

Note: When you log on to the Web UI with the temporary certificate, you are warned that the certificate is not signed or authenticated. Permit the use of the temporary certificate only during initial configuration, when the system is not attached to active networks that could be a source of attack. Install a signed and authenticated certificate prior to connecting any untrusted network.

4 Enter **`apply`** to apply the changes.

End of Procedure

Result: Secure HTTP is now enabled and a certificate is generated. A PC on the Intranet can now use HTTP to access the Web UI on the SMC.

Defining the remote access list

You can remotely manage the SMC using Telnet, SSH, or the Web UI. For security purposes, access to these features is restricted through the remote access list.

Using the remote access list, you can specify IP addresses or address ranges that are permitted remote access to the system. There is only one remote access list, which is shared by all remote management features.

If a client whose IP address is not on the list requests remote management access, the request is dropped. By default, the access list is empty, meaning that all remote management access is initially blocked.

IMPORTANT!

Nortel recommends that you add trusted management clients to the access list when initially enabling any remote management feature. It is also vital that you review the access list regularly and keep it up to date.

Displaying the access list

The following CLI command is used to view the access list:

>> # /cfg/sys/accesslist/list

Adding items to the access list

Procedure 21
Adding items to the access list

1 Start a console terminal.

2 Press <Enter> on the console terminal to establish the connection.

The SMC login prompt appears.

3 Enter **admin** for the login name.

4 Enter the Admin user password.

5 Enter **/cfg/sys/accesslist** to select the Access List menu.

You can repeat the add command to add more remote clients as required. For example, to allow IP addresses 201.10.14.7 and 214.139.0.0/24 to access remote management features, use the following commands:

```
>> # /cfg/sys/accesslist(Select access list menu)
>> Access List# add 201.10.14.7 255.255.255.255(Add
single address)
>> Access List# add 214.139.0.0 255.255.255.0(Add
range of addresses)
```

6 Enter **<base IP address to permit> <network mask for range>** to add a trusted remote IP address to the list.

Note: Although you can enable and disable each remote management feature (Telnet, SSH, and Web UI) independently, all share the same access list. All addresses on the access list are permitted to access any enabled management feature. You cannot enable SSH for some and Telnet for others.

7 Enter **apply** to apply the changes.

End of Procedure

Result: The access list is defined. You can now log on to the SMC at any workstation whose IP address is on the access list. Using the Web UI, you can continue configuration of the SMC system.

Setting up the Web browser

By default, most Web browsers work with JavaScript and require no additional setup. Check the features and configuration of your Web browser to make sure JavaScript is enabled.

Starting the Web UI

Procedure 22
Starting the Web UI

1 Start a Web browser on a PC that is using an IP address included in the Access List created in Procedure 21 on page 110.

2 Enter one of the following in the Address field of the Web browser:

- host IP address
- host IP address as a name, provided that the IP address is assigned a name on the local domain name server
- cluster MIP address
- virtual IP address.

The SMC login window appears.

Figure 21
SMC Web UI login page

3 To log on, enter the account name and password for the system administrator or operator account. For more login and password information, see "Users and passwords" on page 166.

Note: Expect a delay of a few seconds while the default page collects data from all of the cluster components. Do not stop the browser while loading is in progress.

End of Procedure

Result: You are logged on to the Web UI. To continue the deployment process, you must continue as follows:

- For a stand-alone configuration, continue with "Firewall deployment" on page 77.
- To set up a High Availability configuration, continue with "Installing the redundant SMC" on page 118.

The following sections provide useful information that can help you as you continue the deployment process:

- For an overview of Web UI tasks, see "Global command buttons" on page 113.
- To learn how to save and restore the SMC configuration, see "Saving and restoring the SMC configuration" on page 115.

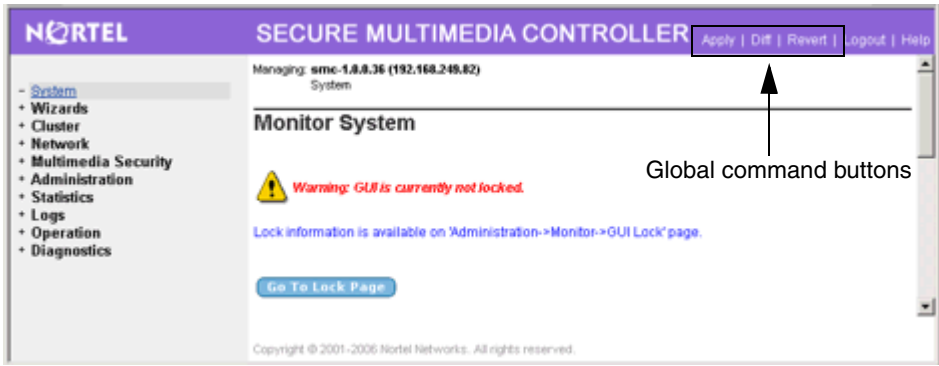
Global command buttons

The global command buttons are always available at the top of each form. These commands summon forms used for:

- saving, examining, or canceling configuration changes
- logging out

Figure 22 identifies the location of the global command buttons.

Figure 22
SMC Web UI components



Web UI task summary

In general, you would perform Web UI tasks in the following order:

1 Create a configuration. See Procedure 23.

2 View pending changes. See Procedure 24.

3 (Optional) Clear pending changes. See Procedure 25.

4 Submitting changes. See Procedure 26.

Procedure 23
Creating a configuration

1 Select the appropriate menu item and sub-page.

2 Modify fields in the appropriate forms display areas.

3 Click **Update** to submit the changes to the pending configuration.

End of Procedure

Procedure 24
Viewing pending changes

1 Click the global **Diff** button.

2 View the **Diff** form.

3 Click **Back** to return to the current form.

End of Procedure

Procedure 25
Clearing pending changes

1 Click the global **Revert** button.

Note: You cannot use the global Revert command to restore the previous configuration after you use the Apply command.

2 Close the browser.

End of Procedure

Procedure 26
Submitting changes

1 Click the global **Apply** button.

Note: Using the Apply command, you can put updates on multiple forms into effect all at once. The Apply function validates the changes to the configuration before applying them, and Apply fails if invalid settings are used. To prevent conflicts, any user logged on as administrator can take control of the GUI lock before changing or creating a configuration.

2 Click **Submit**.

End of Procedure

Saving and restoring the SMC configuration

Periodically, it is necessary to upgrade or reinstall the SMC software. Before doing so, Nortel recommends that you save the existing configuration using the either the Web UI or the CLI.

Procedure 27
Saving the current configuration using the Web UI

1 Using a Web browser, enter the URL to the Web management interface.

The SMC login prompt appears.

2 Enter the administrator account and password.

3 Enter **`admin`** for the default login name.

4 Enter the Admin user password.

5 On the left side of page, click **Operation**.

The Operation Menu expands

6 Click **`Configuration`**.

The Export Cluster Configuration section of the page contains the configuration data.

7 Enter a password to be used to encrypt sensitive data in the configuration file. You will need this password to be able to restore the configuration later.

Note: Nortel recommends that you record the password used to encrypt sections of the configuration file.

8 Click **Export**.

The File dialog box is displayed.

9 Select the location to store the file.

10 Specify a file name.

11 Click **Ok**.

End of Procedure

Result: The configuration is downloaded and saved in the file at location specified. You can view the configuration using a standard text editor.

Procedure 28
Enabling TFTP

TFTP and FTP are disabled by default. If you want to use TFTP or FTP to save or restore the configuration, the TFTP ALG needs to be enabled.

1 Enter **`/cfg/smc/settings/alg/tftp y`**

End of Procedure

Result: The TFTP ALG is enabled. The Web UI does not use TFTP; however, you can turn on the TFTP ALG in the Web UI at the **Multimedia Security > Security Settings > ALG > TFTP** page.

Procedure 29
Saving the current configuration using the CLI

1 Enter **`/cfg/ptcfg`** to start the save (put) configuration wizard.

2 Select the protocol when prompted. The default is TFTP.

The protocol options are: TFTP, FTP, SCP, or SFTP.

3 Enter the hostname or IP address of the server.

4 Enter the filename on the server for the uploaded configuration.

5 Enter a password for selected data in the configuration file.

Secure parameters such as passwords are encrypted with this value. The password must be at least 4 characters.

End of Procedure

Result: The configuration is downloaded and saved in the file at location specified. You can view the configuration using a standard text editor.

Procedure 30
Restoring the current configuration using the Web UI

1 Using a Web browser, enter the URL to the Web UI.

The SMC login prompt appears.

2 Enter the administrator account and password.

3 On the left side of page, click **Operation**.

The Operation Menu expands

4 Click **Configuration**.

5 In the Import Cluster Configuration section of the page, enter the key to encrypt the data.

6 Choose one of the following:

- Enter the full path to the configuration file.
- Click **Browse** and navigate to the file.

7 Enter the secret key that you used to export the configuration.

8 Click **Import**.

The following warning is displayed:
`Importing a configuration will restart the Web server. Are you sure you want to continue?`

9 Click **Ok**.

The Web session is logged off and you are returned to logon page.

10 Log on to the SMC again.

End of Procedure

Result: The restored/imported configuration is now active.

Procedure 31
Restoring the current configuration using the CLI

1 In the CLI, enter **`/cfg/gtcfg`** to start the restore (get) configuration wizard.

2 Select the protocol when prompted. The default is TFTP.

The protocol options are: TFTP, FTP, SCP, or SFTP.

3 Enter the hostname or IP address of the server.

4 Enter the filename on the server for the uploaded configuration.

5 Enter a password for selected data in the configuration file. This password was entered when configuration was saved

End of Procedure

Result: The restored/imported configuration is now active.

Installing the redundant SMC

To set up a High Availability SMC cluster using a redundant SMC, the following conditions are required:

- Install and configure the primary SMC with basic parameters, as described in Procedure 18 on page 102, and then running through any additional setup.
- Fill in the“SMC network engineering worksheets” on page 99.
- Make sure the second SMC has the same hardware and software image as the first SMC. You cannot mix different models or software versions in the same cluster. All ports and security zones must also match across each device.
- Set the redundant SMC to factory default configuration. If the SMC is new, or was just installed from an .ISO or an .IMG file, it is already in factory default mode. You can tell that an SMC is in factory default mode if when you log on as "admin", the menu displays the following command choices: new or join.

- Make sure that the layer 2 switch connecting the different networks between the two SMCs provides redundant network feeds to both SMCs. The switch or hub must also be able to forward multicast packets. The layer 2 switch must not run Spanning Tree Protocol (STP) because STP interferes with the VRRP processes.
- Connect each of the SMC management ports to each other by a single cable.
- Make sure an access list entry is present for the management/cluster network. Otherwise, when the new SMC tries to join with the existing one, it does not have network access. To view the access list:
  - CLI: **`/cfg/sys/accesslist`**
  - Web UI: **Administration > Access List**

Procedure 32
Installing the redundant SMC

1 Make sure that the first SMC is on and operational.

2 Rack-mount the redundant SMC hardware. See “Hardware installation” on page 59.

3 Connect the power cable for the redundant SMC, but do not turn it on yet. See “Hardware installation” on page 59.

Note: Be sure to connect each network to the same port/interface on both SMCs. Each SMC must have identical network connections.

4 Connect the ports of both SMCs to their respective subnets. See “Hardware installation” on page 59.

End of Procedure

Procedure 33
Preconfiguring the first SMC

It is often helpful to pre-configure the first SMC with the IP addresses used on the second SMC prior to adding the second to the cluster. Preconfiguration allows the second SMC to immediately set the IP addresses after the two SMCs join and limits the number of error messages generated when the device starts up.

In a HA configuration, three IP addresses are used for each cluster interface. One IP address per interface is defined for each SMC device in the cluster, and a third is a floating Virtual IP used by the routers for directing traffic. You can specify these values and apply prior to actually joining the second device to the cluster. These additional values are ignored until High Availability is turned on.

1 On the first SMC, start a console terminal and login as admin.

2 For each Interface in the cluster, except management, specify two additional IP addresses -- one for the physical interface on the second SMC, and a second as a virtual router IP. The example in this procedures shows how to set the IP address of the physical interfaces and virtual IP on the intranet zone. All three addresses need to be in the same subnet. Each zone further needs to have a unique virtual router id.

   - CLI command sequence:
     `/cfg/net/if intranet/ip2 n.n.n.n`
     `/cfg/net/if intranet/vrrp/vip n.n.n.n`
     `/cfg/net/if intranet/vrrp/vrid 1`
   - Web UI command sequence:
     Multimedia Security > Security Zones > intranet > Interface > IP Address for Host 2
     Multimedia Security > Security Zones > intranet > Interface > Virtual IP
     Multimedia Security > Security Zones > intranet > Interface > Virtual Router ID

   Note: Each virtual router interface gets a unique vrid, which is used to generate the virtual router MAC address.

3 Repeat the command in step 2 for the TLAN, ELAN, MSCLAN, and Server LAN subnets as configured.

4 Apply the changes:

   - CLI: Enter **`apply`**
   - Web UI: Click **apply**.

End of Procedure

Result: The first SMC is preconfigured. You can now join the two SMCs.

Procedure 34
Joining the second SMC

1 Power on the redundant SMC.

2 Start a console terminal.

3 Press <Enter> on the console terminal to establish the connection.

Result: The SMC login prompt appears.

4 Enter **`admin`** for the default login name.

5 Enter **`admin`** for the default password.

6 Enter **`join`**

7 Enter the basic configuration parameters as requested. The join process can take several minutes to complete.

End of Procedure

Result: The SMCs are joined. Because the system is now an SMC cluster, all configuration is shared across both SMCs. So redundant SMC now has the same configuration as first SMC. Modifying one SMC propagates changes to the other SMC automatically.

To complete the High Availability installation, you must now enable the VRRP processes.

Procedure 35
Enabling High Availability

1 Log on to either the first SMC or the redundant SMC.

2 Turn on High Availability.

- CLI: **`/cfg/net/vrrp/ha y`**
- Web UI: **Network > VRRP > High Availability**

3 Apply the changes:

- CLI: Enter **`apply`**
- Web UI: Click **apply**.

4 Validate that the cluster is running VRRP.

- CLI: **`/info/net/vrrp/status`**
- Web UI: **Main System Page** at the top of left-hand menu

End of Procedure

Result: The SMC cluster is now in High Availability Mode. All packets are now being directed to the Virtual IP addresses.

To continue the deployment process, continue to “Firewall deployment” on page 77.

Secure UNIStim deployment

Contents

This chapter contains information about the following topics:

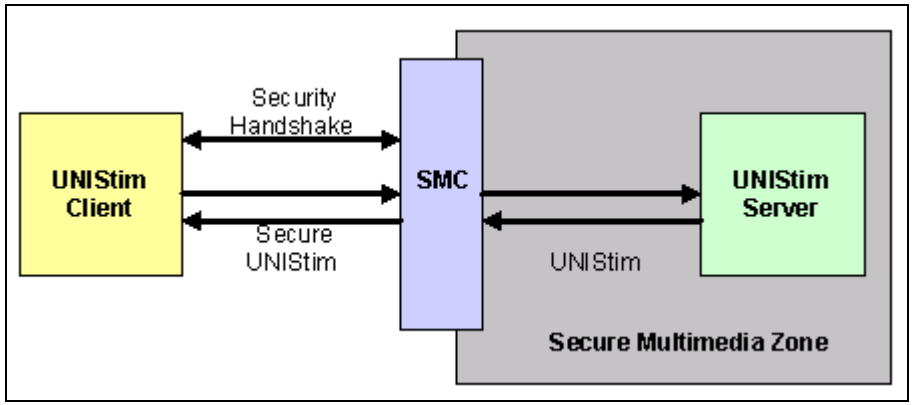
Introduction

UNIStim is a Nortel-proprietary signaling protocol used within the MCS and CS 1000 product lines. Using UNIStim, a UNIStim IP Phone communicates with a UNIStim server (TPS) using the User Datagram Protocol (UDP).

> ***Note:*** The SMC currently supports Secure UNIStim for the CS 1000 but not for the MCS 5100.

The SMC acts as a Secure UNIStim proxy; it terminates the Secure UNIStim handshake from the UNIStim client and then communicates with the back-end server using insecure UNIStim. The proxy is transparent, meaning that neither the client nor the server recognize the SMC is handling the connection. The client talks directly to the server, and the server communicates with the client. Figure 23 on page 125 illustrates Secure UNIStim.

Figure 23
Secure UNIStim overview



IMPORTANT!

Because the SMC is a transparent proxy, you do not need to change the server IP address that you specified during client configuration when you added the SMC to the network. The client continues to communicate with the server as it previously did.

Security policy

By default, the SMC defines a security policy for all clients. This is not visible in the Secure UNIStim configuration wizard but you can change or enhance the security policy from the **Multimedia Security > UNIStim Security > Client > Policy** page of the Web UI.

Each policy is tied to a subnet or a set of subnets upon which the clients reside. You can specify a single client with a 32-bit mask. You can associate different policies to individual client groups.

Configuration options for security policies:

- Upgrade to secure session: Tries to convert an insecure session to a secure session.

- Require client security: Allows only secure sessions and denies all insecure sessions.
- Enable session caching: Provides a quicker handshake if the phone restarts. Nortel recommends session caching.
- Key renewal: Specifies renewal intervals for the different keys used in the handshake.
- Firmware check: Enables the SMC to consult the IP Client Firmware table to confirm that the IP Phones support UNIStim security for new connections. Nortel recommends firmware checking if you have a heterogeneous mix of IP Phones, including IP Phones that do not support security.
- Automatic fingerprint update: Updates the fingerprint on clients that were never configured for security. Automatic fingerprint updating runs when the SMC is first inserted into a network so that you do not need to manually configure the IP clients.
- Security in External Redirections: Maintains the current security level in redirections to external servers,.

By default, the SMC keeps all IP client in an insecure mode. This allows the administrator to control the Secure Unistim roll-out so that licences are not exceeded.

IMPORTANT!

To add enhanced security for all IP Phones protected by a given policy, client security is required. UNIStim phones with firmware that does not support security, such as the IP Softphone 2050 and the WLAN handsets 2210 and 2211, needs a policy that does not require UNIStim security. See “Security policy example” on page 127 for an example of how security policies work.

For these phones, set the policy to **Required Security = false**. These unsupported IP Phones are then allowed to pass through as unsecure, even though the SMC tries to upgrade them. For more information about unsupported IP Phone firmware, see “IP client firmware management” on page 156.

When the SMC is first installed, three standard policies are created:

- insecure: does not try to upgrade phones to Secure UNIStim or push the key fingerprints to the IP Phones.
- secure: tries to upgrade IP Phones that are not configured for security to Secure UNIStim and push the key fingerprint of the primary key to the IP Phone. Any IP Phones that do not support security are allowed to access the Signaling Server using normal UNIStim.
- maxsecure: this policy works the same as secure, except that IP Phones that cannot be upgraded to security are denied access to the Signaling Server.

The default rule in the SMC maps a network called voip_users to a nonsecure Policy. The Client Rules can be viewed in the Web UI at:**Multimedia Security > UNIStim Security > Client > Rules.**

Security policy example

In this example, the Finance Network requires a high level of security (the secure policy), while Sales requires less security (the nonsecure policy).

Figure 24 illustrates a group of IP clients, the subnet they are on, and the SMC network name that has been given to those clients. Figure 25 on page 129 shows, in the Web UI, how the IP client network is tied to the policy and Figure 26 on page 130 shows group of IP clients that does not support secure UNIStim.

Figure 24
Security policy diagram

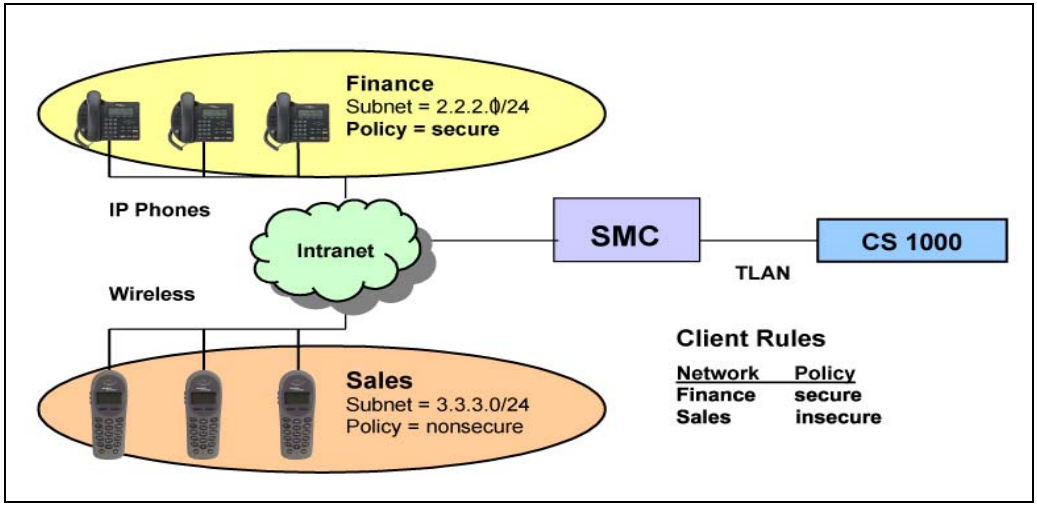


Figure 25
Sample policy page

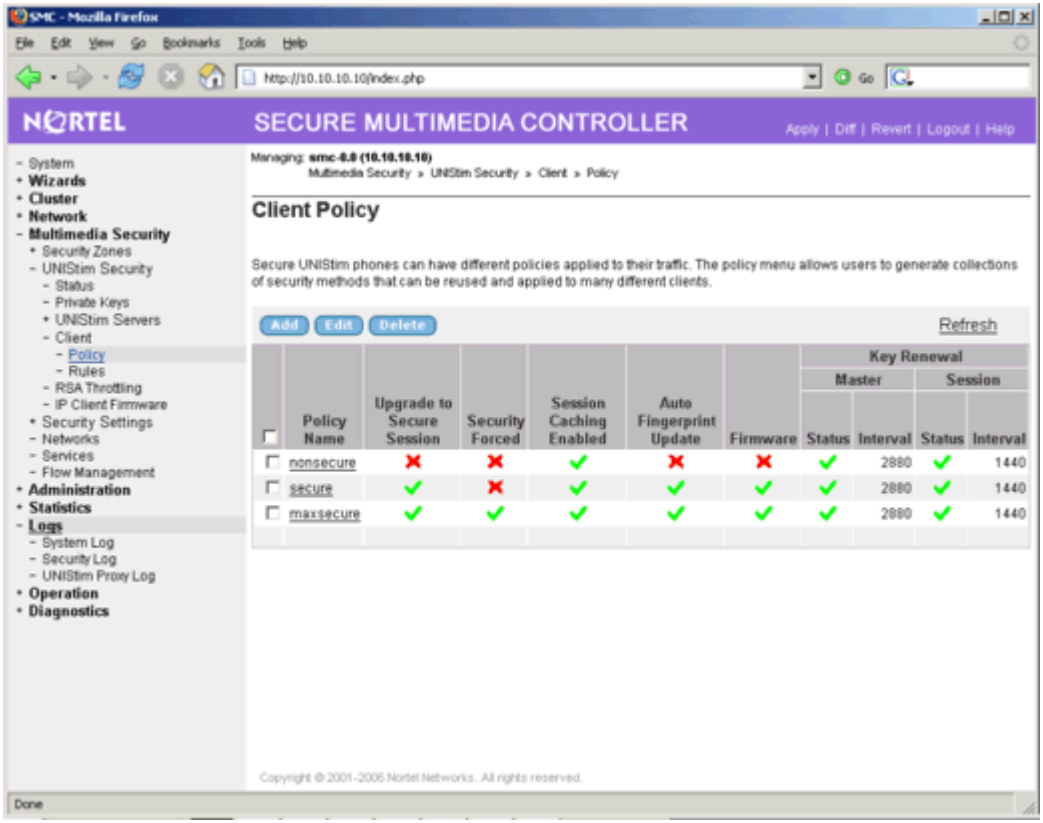
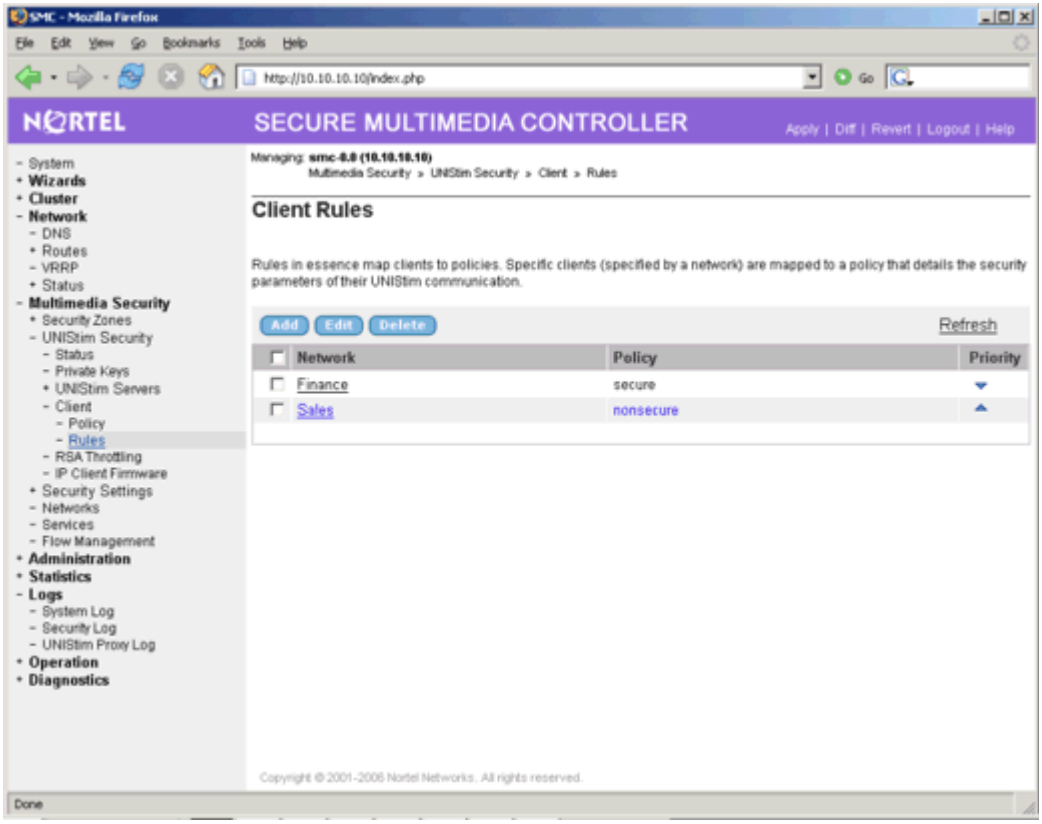


Figure 26
Sample rules page



Security in External Redirections feature

When an IP Phone is redirected to a server that is not located in an SMZ protected by the current SMC, the Security in External Redirections feature determines how the action byte is set. If the action byte is 1 (insecure), the IP

Phone is redirected insecurely. If the action byte is 6 (secure), the phone is redirected securely.

Table 12 identifies the default Security in External Redirection settings for a new SMC installation.

Table 12
Default Security in External Redirection settings

Policy	Default setting
nonsecure	disabled
secure	disabled
maxsecure	enabled
custom policy	enabled

WARNING

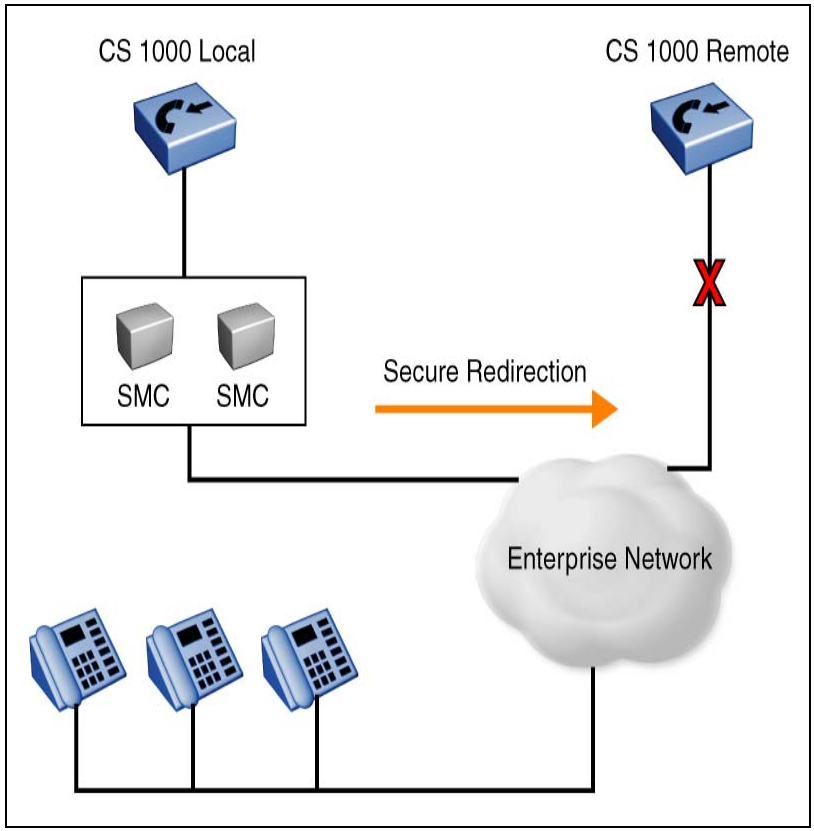
Disabling the Security in External Redirections feature on a custom policy leaves the IP Phone open to a man-in-the-middle attack.

Security in External Redirections feature in Virtual Office

The Security in External Redirections feature is important for features such as Virtual Office. If the Security in External Redirections feature is enabled and the phone is connected securely, the IP Phone is prompted when it is redirected to make a secure connection to the external server. If the external server is not protected by an SMC, the phone connection fails with a security error.

As illustrated in Figure 27, if the phones are communicating securely with CS 1000 Local and then are securely redirected to CS 1000 Remote, the IP Phone connections fail because the CS 1000 Remote is not protected by an SMC and therefore does not support security.

Figure 27
Virtual Office redirection scenario



Note: Even if both servers are protected by SMCs, the redirection may still fail if the IP Phone does not have a fingerprint that matches the second server.

IMPORTANT!

In a Virtual Office configuration configuration in which all Signaling Servers are not protected by an SMC, Nortel recommends that you disable the Security in External Redirections feature so that the IP Phones are redirected insecurely to CS 1000 Remote and they can establish connectivity; however, this methodology is not fully secure.

To support a fully secure Virtual Office installation, you must install SMC devices in front of each CS 1000 Signaling Server and enable the Security in External Redirections feature for all IP clients. Furthermore, the keys on each SMC device must be the same, so the IP clients can establish connectivity.

First-time deployment

Nortel recommends that Secure UNIStim be enabled on a small group of target users first to ensure the process is understood. After operation has been confirmed for a couple of days, the Policies or Network definitions can be changed to include additional IP clients.

IMPORTANT!

Prior to deploying Secure UNIStim, install the supported firmware image on all IP Phones served by the SMC.

Turn on the default Secure UNIStim policies for an initial deployment. The policies try to upgrade IP Phones to security (but does not require it) and automatically add the public key fingerprint to any phones were never configured for security.

When Secure UNIStim is turned on the first time, all proxied secure and insecure UNIStim connections are re-established and their current calls are dropped.

Configuring Secure UNIStim

The Secure UNIStim wizard in the Web UI guides you through the baseline procedure to enable UNIStim security, create a private key for encryption, select the policy, and specify the UNIStim servers to be proxied.

WARNING

Enabling Secure UNIStim causes all phones communicating with configured UNIStim servers to reset and reconnect through the SMC. Because of this, enable Secure UNIStim only during a maintenance window. It generally takes between 3 to 5 minutes for phones to reset.

Procedure 36
Configuring Secure UNIStim

1. Login to the Web UI.
2. Navigate to the following page:
   Wizards > Configure > Secure UNIStim

   The Secure UNIStim Wizard page is displayed.
3. Read Wizard instructions on page.
4. Select **Yes** to enable Secure UNIStim.

   Note: Turning on Secure UNIStim causes all IP Phones using Secure UNIStim proxied servers to reset and re-establish connectivity.
5. Click **Next**.
6. Select **Yes** to create the primary key.
7. Enter a name for the private key.

   This name is used in the configuration to define the primary key. Key names must start with a letter and consist of letters and numbers. Since the fingerprint for this key is stored on all IP Phones, export and store this key after the wizard has completed.
8. Click **Next**.
9. Select **Yes** to add UNIStim servers.
10. Add the servers.

    Note: Currently only CS 1000 Signaling Servers are supported. You can add up to five servers on this page. You can add more servers as part of the standard SMC configuration.
11. Click **Finish**.
12. View the final page.

    Note the key fingerprint displayed on the screen. This fingerprint needs to be stored on the IP Phones before they can communicate with the SMC. You can key the fingerprint into the IP Phone manually or the fingerprints can be automatically set on the IP Phones by the SMC if automatic key update is enabled in the Client Policy.
13. Add the UNIStim Rule to upgrade phones to security.

By default, the voip_users network matches all subnets so all traffic flowing through the SMC is insecure. To segment out a particular network for security, you must perform the following steps:

a. Add a network for the subnet(s) you want to secure. Networks are added in the Web UI at the **Multimedia Security > Networks** page.

b. Create a rule by associating the network to a policy. Rules are applied in order of display and since the default rule matches all networks, it is always called if it is first in the list. You will need to re-order the Rule list to place the new more restrictive Rule first.

14 Extract the private key to a secure location.

a. Navigate to the **Multimedia Security > UNIStim Security > Private Keys** page**.**

b. Select the key to display.

c. Click **Display Private Key/Public Key/Fingerprint**.

d. Click **Private Key**.

You are prompted to specify a password. The password is optional but recommended since this key is critical for communication with all Secure UNIStim phones proxied by the SMC. This password is required when the key is imported back into the SMC.

e. Specify a password.

f. Cut and paste the key into a file for storage.

IMPORTANT!

Maintain the private key in a safe location. It may be needed for another SMC install.

15 Click **Apply**.

Now the SMC is ready to transparently proxy connections from a UNIStim IP Phone to the primary servers entered within the wizard. It may take one minute for the SMC to start handling connections in an HA environment.

IMPORTANT!

If any phones on secure subnets do not explicitly support Secure UNIStim, enable Firmware Checking in the policy. See “Firmware checking” on page 158.

16 To verify that the servers are added correctly, navigate to the **Administration > Monitor > UNIStim Security > Server** page.

This page displays both primary servers and secondary servers separately for each SMC in a HA cluster.

IMPORTANT!

If all servers are not present on server page, the SMC is unable to find a route for them. Examine the System Log (**Logs > System Log**). See “System Log” on page 213.

17 To examine the clients, navigate to the **Administration > UNIStim Security > Clients page**.

18 Prime the SMC using an IP Client.

IMPORTANT!

Because most phones are currently communicating with secondary servers, the secondary servers need to be added to the SMC dynamically. Phones that currently maintain sessions to these secondary Servers do not use the SMC proxy unless these servers are added to the secondary server database. This is done by initiating requests to each of the primary servers and then allowing the SMC to auto-discover the secondary servers.

In this step, an IP Client is programmed to communicate with each Primary UNIStim server in the servers list. When this IP Client is redirected to the various secondary servers, those servers are added to the SMC Dynamic Servers list.

Note: In some installations, load balancing is used in the server redirections. Load balancing makes the servers non-deterministic and the client may not be able to prime the system with all secondary servers in a single run.

If, after 3 to 5 minutes, all known servers are added and there are still IP Phones that have not been redirected through the SMC, you should reset the phones from the Element Manager for the Signaling Server. This reset forces them to start from the initial primary servers, and all redirection pathways are captured by the SMC.

You can monitor the server additions through the UNIStim Servers page.

19 Examine the IP Clients after priming the Secondary Servers.

The UNIStim Clients page has additional entries. Each entry details whether the client is secure, how many redirections it has experienced, and a listing of the client firmware type.

IMPORTANT!

You can troubleshoot problems with IP Client connectivity by examining the Secure UNIStim log in the Web UI at: **Logs > UNIStim Proxy Log**.

The UNIStim Proxy Log page displays critical security errors and allows you to search for individual clients by entering the client IP address into the search field.

20 Update the License.

If you have not yet added additional licenses to the SMC, you can add them while the SMC is running. Each device in a HA cluster requires a separate license.

a. Obtain the MAC address of the SMC from the **Cluster > Host(s) > License** page.

Each host in a HA cluster will have a different MAC address. The MAC address internally maps to port 1.

b. Obtain the license from Nortel.

c. Paste the license into the **New License** window and save it. Repeat this step for each SMC for each host in a HA cluster. It takes approximately 30 seconds before the license goes into effect.

End of Procedure

Result: Secure UNIStim is enabled on the SMC.

Viewing the security keys

Using the Web UI, you can view the public key/private key/ public key fingerprint for a generated key.

Procedure 37
Viewing the security keys

1. Log on the Web UI.
2. Navigate to the **Multimedia Security > UNIStim Security > Private Keys >Display private key/public key/fingerprint** page.
3. Select one of the following options to display the generated keys:
   - Private Key
   - Public key
   - Public key fingerprint

End of Procedure

Result: The security key is displayed.

Verifying the IP Phone connection

Using the Web UI, you can check whether a phone is connected in secure or non-secure mode.

Procedure 38
Verifying the IP Phone connection

1. Log on the Web UI.
2. Navigate to the **Administration > Monitor > Unistim Security > Client** page.

End of Procedure

Result: The page displays all the connected phones with IP addresses, firmware details, and whether it is in secure or non-secure mode.

Troubleshooting Secure UNIStim

When Secure Unistim is enabled on the SMC, the change of IP Clients from insecure to secure does not happen immediately. You can view the IP client security status at the **Administration > Monitor > UNIStim Security > Client** page in the Web UI.

The following section explains why Secure UNISTIM reregistration can be delayed and how to speed the process up.

When an insecure IP Client is rebooted, it goes through the following process:

1 The phone communicates to the CS 1000 Node IP address on port 4100.

2 The Node TPS redirects the IP Client to either:

- the TLAN IP of the same Node TPS
- another TPS device TLAN address (load balancing process)

3 The IP Client communicates to the TPS TLAN IP at the supplied address on port 7300

4 After registration completes, the IP client communicates to the same TPS as step 3 on TLAN IP port 5100

The IP Client is now registered and ready to operate.

Note: The 4100/7300/5100 port numbers are factory default.

When secure UNIStim is disabled and phones are operating normally, the phones operate in the final state, as identified in step 4.

When security is enabled, the SMC firewall is designed to do the following for both secure and insecure IP Clients:

- recognize that an IP Client is communicating to the CS 1000 Node address on port 4100. During the configuration of the Secure UNIStim feature on the SMC, the TPS server IP address is provided.
- watch IP client communications move to the assigned TPS TLAN address using port 7300
- watch the IP client finish registration on port 5100
- track this activity using a firewall-based client table

When secure UNIStim is enabled on the SMC, the phones are most likely still in step 4; therefore, the firewall does not get the opportunity to track the IP client through the registration process.

How to speed up the transition from insecure to secure UNIStim:

- if the CS 1000 has a single TPS, reboot an IP Phone. This reboot creates a firewall entry that has: `<Node-IP:4100>-<TLAN-IP:7300>-<TLAN-IP:5100>`. This causes all other telephones registered to <TLAN-IP:5100> to reconnect to the SMC in secure mode.
- if the CS 1000 has multiple TPS servers, reboot multiple phones that are load shared across multiple TPS servers. Through load sharing, the various TPS servers are discovered.
- to push all phones immediately during a maintenance window, reset all phones through Element Manager on all TPS servers.

Configuring the IP Phones

Table 13 on page 142 lists the IP Phones supported by the SMC and identifies whether they are supported by the Secure UNIStim Proxy. Unsupported IP Phones need to traverse the SMC insecurely using a policy that does not require security.

Table 13
Supported IP Phones

IP Phone	Secure UNIStim	Insecure UNIStim
IP Phone 2001 (Phase 2)	Yes	Yes
IP Phone 2002 (Phase 2)	Yes	Yes
IP Phone 2004 (Phase 2)	Yes	Yes
IP Phone 2007 (Phase 2)	Yes	Yes
IP Phone 1110	Yes	Yes
IP Phone 1120E	Yes	Yes
IP Phone 1140E	Yes	Yes
IP Softphone 2050	Yes	Yes
WLAN handset 2210	**No**	Yes

Table 13
Supported IP Phones

IP Phone	Secure UNIStim	Insecure UNIStim
WLAN handset 2211	**No**	Yes
IP Audioconference Phone 2033	Yes	Yes

IMPORTANT!

All IP clients protected by a Secure UNIStim policy that necessitates security must have an appropriate firmware image. Some older images have incomplete support for security and, while they can run with secure UNIStim, they may not work as intended.

See the release notes for the current supported images. For release notes, click the Technical Documentation link under Support & Training on the Nortel home page:

www.nortel.com

Enable security

By default, IP Phones run in an insecure state. To manually enable security, you must turn security on using the phone keypad on each IP Phone. This is not practical when there are many IP Phones in the enterprise. In large installations, Nortel recommends the server auto-update. The following section describes the manual configuration of security.

Enable security on the SMC

Enable security on the SMC for the server to which the client connects. For more information about UNIStim, see “Secure UNIStim deployment” on page 123.

Configure the IP Phones for security

Procedure 39

Configuring the IP Phone 2001, IP Phone 2002, or IP Phone 2004 for security

1. Choose one of the following:
   - For the IP Phone 2001, IP Phone 2002, or IP Phone 2004 , turn on or reboot the IP Phone and then press the four soft tabs at the bottom of the screen, once each from left to right, to enter the configuration menu.
   - For the IP Phone 2007, click the Setting button on the left corner of the screen and then select Network Configuration
2. Press the **OK** softkey to bypass many entries until the first Action Byte prompt appears.
3. Change the action byte from 1 (insecure) to 6 (secure).
4. Set the RSA public key fingerprint using the 16-byte fingerprint corresponding to the public/private key pair stored on the SMC.

   Note: The Fingerprint prompt (S1 PK) is only presented if the action byte is 6.

   The RSA public key fingerprint is retrieved from the Web UI or CLI and is associated with the primary key of the server. It consists of sixteen hexadecimal digits (0 - 9 and a - f). You must manually enter the RSA public key fingerprint into the IP Phone. An example 16-character fingerprint is: 8a166e6cc08be496. Key in the numerals (0 - 9) using the phone keypad. Key in the letters using the convention of the pound key (#) plus the corresponding number. For example, #1 = a and #6 = f.
5. If the IP Phone can register to an alternate server (S2 IP), change the action byte and key fingerprint as required for S2.
6. Press the **Apply and Reset** button.

End of Procedure

IMPORTANT!

For Phase 2 IP Phone 2001/IP Phone 2002/IP Phone 2004, you can set the RSA public key fingerprint after the action byte is set to 6 for either the S1 or S2 servers. The key fingerprints, however, are not tied to either of the S1 or S2 servers even though it may appear this way during the configuration. Instead, the two allowed fingerprints are treated as a pool of fingerprints; either one can authenticate S1 or S2

WARNING

The automatic update feature is available for IP Phones that do not have security configured. After the RSA public key fingerprint or the action byte is set, the initial key automatic update directed by the SMC no longer works.

Automatic update is different than the fingerprint update in that the automatic update occurs when the back-end SMC changes its primary key to a secondary key. In fingerprint update, the current fingerprint on the IP Phone, which corresponds to the secondary key, is overwritten with the new fingerprint of the primary key.

If the IP Phones have an old fingerprint but you want to use the automatic update feature, you must manually configure the public key fingerprint to “ffffffffffffffff” when you configure the IP Phones for security. See “Configure the IP Phones for security” on page 144.

Procedure 40
Configuring the IP Phone 1140E and IP Phone 1120E for security

IMPORTANT!

Timing information

There are approximately 45 seconds between plugging in the IP Phone power adapter and the appearance of the text Nortel. When you see the text Nortel on the phone, you have 1 second to respond by pressing the four soft keys at the bottom of the display in sequence from left to right, one at a time. If you miss the 1-second response time, the IP Phone attempts to locate the connect server. You can begin the power-up sequence again, or you can double-press the Services key to open the Local diagnostic utilities to access the IP Phone settings.

If you are prompted to enter a password when you double-press the Services key, password protection is enabled.

1. If configuring the first time, power on the IP Phone.
2. When the Nortel logo appears in the middle of the display, immediately press the four soft keys at the bottom of the display in sequence from left to right. The **3. Network Configuration** menu opens.

   Press the **Apply&Reset** soft key to save the following settings and to reset the IP Phone. Press the **Exit** soft key to exit the menu without saving any changes and return to the **3. Network Configuration** menu.
3. Use the **Right** navigation key to scroll and highlight **S1 Action**. Press the **Enter** key to start the edit mode. Use the dialpad to fill in the information. Choose one of the following:
   - for TPS only, enter 1
   - for TPS and Secure Multimedia Controller, enter 6 or 1
4. To change the action byte from 1 (insecure) to 6 (secure), press the **Enter** key, enter 6, and then press the **Enter** key again
5. Use the **Right** navigation key to scroll and highlight **Retry**. Press the **Enter** key to start the edit mode. Use the dialpad to fill in the information:

Retry—the number of times the IP Phone attempts to connect to the server.

6 Use the Right navigation key to scroll and highlight **S1 PK**.

S1 PK—the Private key of the Secure Multimedia Controller to which the IP Phone connects.

7 Press the **Enter** key to start the edit mode.

To manually configure the S1 PK, set DHCP to Partial or None. S1 PK Default is ffffffffffffffff.

Set the RSA public key fingerprint using the 16-byte fingerprint corresponding to the public/private key pair stored on the SMC.

The RSA public key fingerprint is retrieved from the Web UI or CLI and is associated with the primary key of the server. It consists of sixteen hexadecimal digits (0 - 9 and a - f). You must manually enter the RSA public key fingerprint into the IP Phone. An example 16-character fingerprint is: 8a166e6cc08be496.

To enter ALPHA hexadecimal digits, use the IP Phone dialpad to enter the following:

1 = A

2 = B

3 = C

4 = D

5 = E

6 = F

8 Press the **Apply&Reset** soft key.

9 Use the **Right** navigation key to scroll and highlight **S2 IP.** Press the **Enter** key to start the edit mode. Use the dialpad to fill in the information:

S2 IP—the secondary CS 1000 node IP address for the IP Phone.

The IP Phone can support a primary (S1) and secondary (S1) connect server. If you require IP Phones to register on multiple nodes, see *IP Line Fundamentals* (NN43100-500).

10 Use the **Right** navigation key to scroll and highlight **S2 Action**. Press the **Enter** key to start the edit mode. Use the dialpad to fill in the information. Choose one of the following:

- for TPS only, enter 1
- for TPS and Secure Multimedia Controller, enter 6 or 1

11 To change the action byte from 1 (insecure) to 6 (secure), press the **Enter** key, enter 6, and then press the **Enter** key again

12 Use the **Right** navigation key to scroll and highlight **Retry**. Press the **Enter** key to start the edit mode. Use the dialpad to fill in the information:

Retry—same as S1.

13 Use the Right navigation key to scroll and highlight **S2 PK**.

S2 PK—the Private key of the alternate Secure Multimedia Controller to which the IP Phone connects.

14 Press the **Enter** key to start the edit mode.

To manually configure the S2 PK, set DHCP to Partial or None. S2 PK Default is ffffffffffffffff.

Set the RSA public key fingerprint using the 16-byte fingerprint corresponding to the public/private key pair stored on the alternate SMC.

The RSA public key fingerprint is retrieved from the Web UI or CLI and is associated with the primary key of the server. It consists of sixteen hexadecimal digits (0 - 9 and a - f). You must manually enter the RSA public key fingerprint into the IP Phone. An example 16-character fingerprint is: 8a166e6cc08be496.

To enter ALPHA hexadecimal digits, use the IP Phone dialpad to enter the following:

1 = A

2 = B

3 = C

4 = D

5 = E

6 = F

15 Press the **Apply&Reset** soft key.

End of Procedure

Note: If you used automatic fingerprint update and the IP Phones have default configuration value for fingerprint as fffffffff and action byte 1 and you want to check whether correct fingerprint was written to the IP Phones by the SMC, you have to enter the network configuration.

For IP Phone 2002 and IP Phone 2004, you must change the action byte to 6 and then go to the fingerprint menu item. For IP Phone 1140E, IP Phone 1120E and IP Phone 2007, you can look at the fingerprint by scrolling down the configuration menu.

Automatic fingerprint update

For IP Phones running in insecure mode with default security settings, the SMC can automatically update/populate the public key fingerprint on the phone and turn on security. For the automatic update feature to work, you must enable the following two secure UNIStim policy items:

- Upgrade secure session
- Automatic fingerprint update

To disallow the connection if the IP Phone cannot convert to security, enable the *Require security* policy.

IMPORTANT!

Automatic fingerprint update can occur only once: when the IP Phone has the factory default FFFFFFFFFFFFFFFF fingerprint and the Action Byte is 1. To change the fingerprints on the IP Phone a second time, use the SMC private key update feature. This feature generates a connection using the previous fingerprint and then writes the new fingerprint to the phone memory.

IMPORTANT!

Nortel recommends that you export the current SMC private key to a secure location. Encrypt the key when you export it from the SMC. This private key is required for fingerprint updating of the current IP Phones when the primary key changes. Key updating can occur only after a secure session is initiated using the previous key and fingerprint.

For IP Phones that support two fingerprints (such as the phase 2 IP Phones), both fingerprint locations are overwritten with the new key.

Fingerprints on the IP Phones are not tied to the S1 or S2 IP addresses. Instead if one of the two available fingerprints match, the matching fingerprint is used for the handshake. On a fingerprint update directed by the SMC, the fingerprint currently in use is overwritten.

DHCP

Using DHCP, you can initially configure IP Phones and then the IP Phones dynamically retrieve their configuration when they are turned on. You can use DHCP to specify the action byte for the communication. An action byte of 1 means insecure connection and an action byte of 6 means secure connection.

The public key fingerprint cannot be set dynamically through DHCP; however, you can manually set the fingerprint through the phone keypad or automatically set the fingerprint using the SMC automatic fingerprint update feature.

IMPORTANT!

For Automatic fingerprint update to work, the DHCP server must first send an Action Byte of 1. After the SMC pushes the fingerprint to the phone and the SMC shows the phones connecting in Secure mode, the DHCP server can be changed to provide an Action Byte of 6.

Note: Full DHCP provides the capability to change the Action Byte used by the IP Phone. Partial DHCP configures only the IP address, mask, and gateway for the IP Phones and therefore is limited in flexibility.

DHCP recommendations

Nortel recommends that you:

- initially keep the action byte at 1 in DHCP and on the IP Phones so that the automatic fingerprint update can work correctly and push the correct fingerprint to new IP Phones.
- change the default action byte to 6 only when the automatic fingerprint update is no longer needed.

WARNING

If you do not use the automatic update and upgrade features in the Client Policy, but have Require Security in the Client Policy, ensure the DHCP action byte setting is changed to 6 so the IP Phone *always* communicates in secure mode.

Managing the keys

If you have already enabled Secure UNIStim and generated keys using the wizard in Procedure 18 on page 102, the keys are already generated and you do not need to perform the Procedure 41 and Procedure 42.

Before you enable UNIStim security, generate a private key and store it on the SMC. This key, which has a public key associated with it, is used during the security handshake.

For more information about Secure UNIStim keys, see “Key management” on page 37

Procedure 41
Generating or importing the private key

Using the Web UI, you can generate private keys on the SMC device or import private keys. The SMC supports 1024-bit RSA keys. Import of the key is facilitated by the use of PEM encoding, which includes encryption of the key.

1 Log on the Web UI.

1 Navigate to the **Multimedia Security > UNIStim Security > Private Keys > Generate/Set Private Key** page.

2 Choose one of the following:

- Click **Generate**.
- Click **Import** and enter the password if prompted.

Note: This is a unique password and is not associated with the root, admin, or any other password.

End of Procedure

Procedure 42
Exporting the private key

You can export private keys, corresponding public keys, and public key fingerprints from the SMC to a file for storage or transfer to another SMC cluster.

1 Log on to the Web UI.

2 Navigate to the **Multimedia Security > UNIStim Security > Private Keys > Display Private Key/Public Key/Fingerprint** page.

3 Specify a password to encrypt an exported private key.

End of Procedure

Secure UNIStim rules

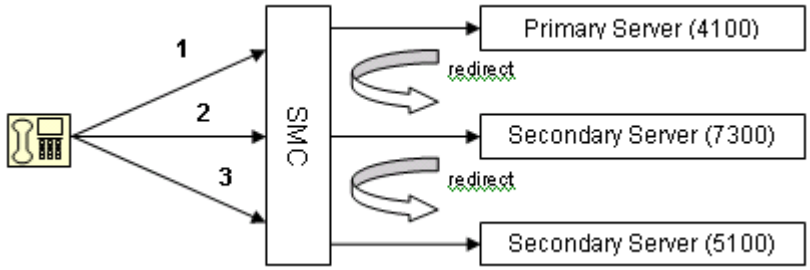
The SMC auto-generates firewall rules for the different security zones that it protects; however, you can customize the firewall rules.

By default, the autogenerated rules allow UNIStim traffic through the SMC for both the CS 1000 and the MCS 5100, enabling insecure UNIStim phones to work by default.

Signaling Servers

CS 1000 signaling sessions typically involve a connection to an initial server, termed *primary* in this document, followed by automatic redirections to *secondary* servers. The primary server typically uses port 4100 and the secondary servers, which can be the same device, typically uses ports 7300 and 5100. In this context, a server is a combination of an IP address and a port. Figure 28 illustrates a standard redirection in a CS 1000 system.

Figure 28
CS 1000 standard redirection



Configure primary server

Only the initial primary server is configured in the SMC. The two secondary servers are automatically discovered and stored persistently in the configuration as dynamic servers. This discovery occurs during the server redirection; if the redirection does not occur, the SMC does not discover these servers.

IMPORTANT!

Only primary servers are configured in the SMC; all secondary servers must be auto-discovered.

Note: Secondary servers can be either additional media cards or Signaling Servers that perform load balancing such as TPS.

Update server database

When secure UNIStim is enabled in an environment with IP Phones already communicating on port 5100 through a firewall rule, there are no appropriate secondary servers to redirect these existing UNIStim sessions.

To assist in automatically populating the secondary servers, reboot a phone to allow the SMC to auto-generate the secondary servers (for ports 7300 and 5100) during redirections. When the server corresponding to the traffic on port 5100 is added to the system, all port 5100 traffic is redirected through the SMC proxy, causing the IP Phones to reset and reconnect according to the SMC security policy.

IMPORTANT!

Secondary servers are propagated to the backup SMC (HA configuration) and stored persistently. The initial database priming is performed only at installation or when the internal server mappings change.

Secondary servers are displayed in the Web UI. You can delete secondary servers but you can not add them. Deleting these servers is discouraged unless the server is not longer in use.

WARNING

After you add the primary servers to the SMC, the IP Phones currently attached to those servers reset and redirect their signaling pathways through the Secure UNIStim transparent proxy. If redirection does not happen in three to five minutes, it can mean that not all secondary servers are added to the SMC configuration. Perhaps the server priming is not complete or the redirection pathways are non-deterministic, such is the case when one server re-directs to multiple other servers, such as for load balancing.

If the IP Phones have not been registered with the SMC, Nortel recommends that you reset the IP Phones directly through the Signaling Server using its management interfaces. The reset redirects the IP Phone back through a primary server and the SMC captures any missed redirections and adds them to its database. Since the servers remain in the database throughout restarts, you only need to reset the IP Phones once when Secure UNIStim is first turned on.

Note: An alternative method is to add the missed Signaling Servers directly to the configuration as Primary Servers.

You can monitor the current state of Secure UNIStim servers and clients in the Web UI at the following pages:

- Primary and Secondary UNIStim Servers: **Administration > Monitor > UNIStim Security > Server**
- IP Phones: **Administration > Monitor > UNIStim Security > Client**

Deleting primary servers

Deleted primary servers are automatically converted into secondary servers to maintain any current connections that exist. To completely remove these servers, you must either restart the SMC or individually remove the servers

using the Servers page (**Administration > Monitor > UNIStim Security > Servers**) page in the Web UI. On the monitoring page, you can see how many connections are currently associated with a particular server. These associated connection are terminated when the server is deleted.

IP client firmware management

The SMC operates in a heterogeneous environment with many different phone types. Some versions of the IP Phone images either support UNIStim security in a limited fashion or do not support UNIStim security at all. Nortel highly recommends that all IP Phones in the SMC-protected network have appropriate Secure UNIStim images.

In some environments, however, Secure UNIStim upgrade is not possible or the current IP Phone image UNIStim security support is present but limited. To protect against IP Phone firmware issues, you can specify which firmware types fully support Secure UNIStim and what level that support includes. You can specify this optional firmware checking in the IP Phone policy.

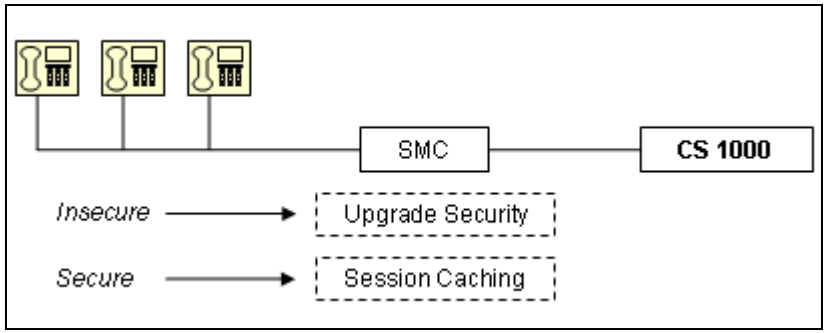
See the release notes for a listing of supported IP Phone firmware. For release notes, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

No firmware checking

If firmware checking is not defined within the IP Phone policy, all IP Phones on the network with signaling that traverses the SMC are treated as if they support security. The SMC handles all IP Phones equally. If upgrade to UNIStim security is enabled, as illustrated in Figure 29, all insecure connections generate an upgrade attempt and all secure connections are available for session caching. If the IP Phone images do not support Secure UNIStim features, attempts by the SMC are ignored and the IP Phones continue to connect insecurely.

Figure 29
No firmware checking

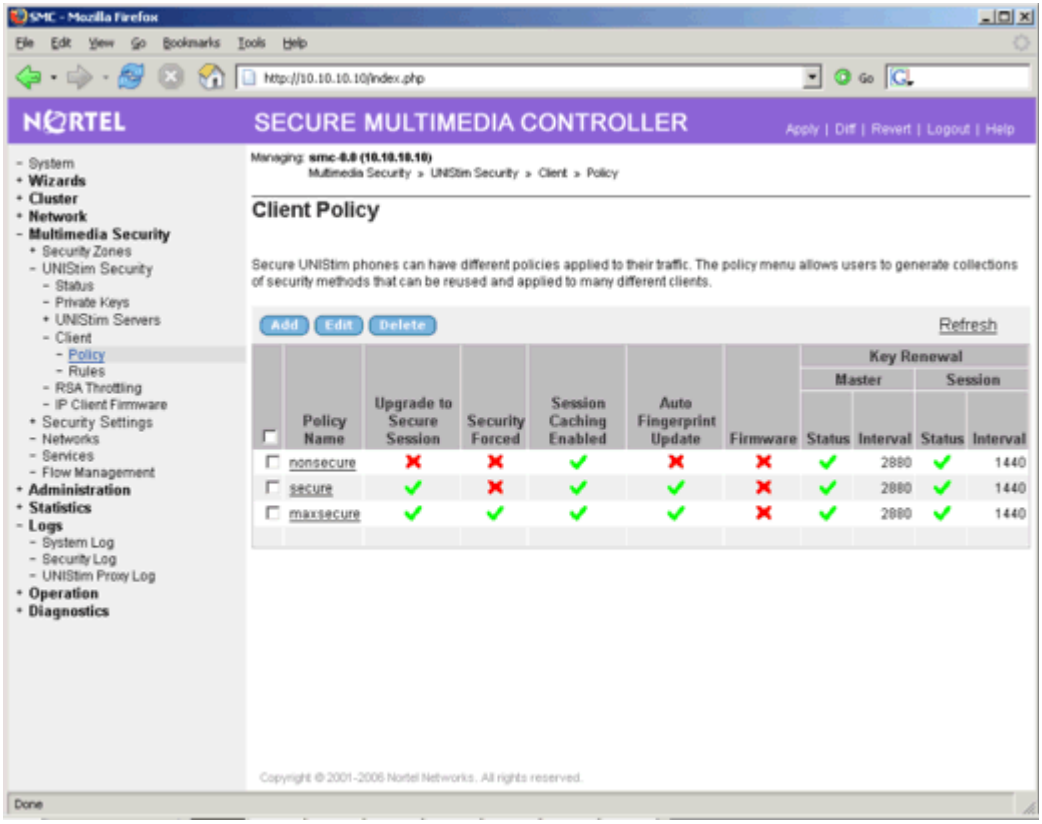


IMPORTANT!

Without firmware checking, older firmware images that support security in a limited fashion are upgraded along with IP Phones running the officially supported IP Phone firmware. Nortel recommends you disable firmware checking only if no legacy Secure UNIStim phones exist on the network.

See Figure 30 on page 158 for examples of the required policies

Figure 30
Sample policies



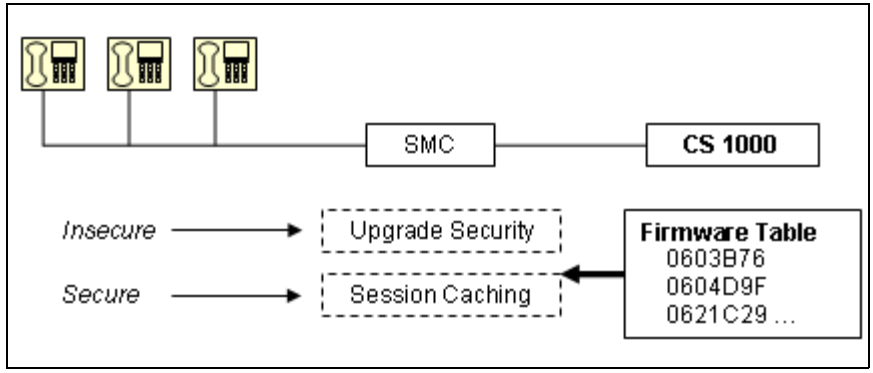
Firmware checking

You set the firmware checking feature in the Secure UNIStim client policy. You can view the IP Phone firmware table in the Web UI at the following page: **`Multimedia Security > UNIStim Security > IP Client Firmware`**.

Using the firmware checking feature, the SMC validates that the IP Phone firmware accurately supports the Secure UNIStim protocol. The SMC handles new IP Phone requests as before the firmware check. However before

upgrading the IP Phone to Secure UNIStim or turning on session caching, the SMC checks the IP Phone firmware to make sure the firmware is supported. If not, the IP Phone request proceeds without intervention by the SMC. See Figure 31.

Figure 31
Firmware checking



IMPORTANT!

IP Phones with images that do not support security are allowed through the SMC only if they match a policy that does not require security.

All IP Phones that generate secure connections to the SMC are allowed to connect securely, whether or not their firmware is supported in the table. The SMC consults the table to determine whether session caching is supported for these connections; however, it does not deny an initial secure request because the IP Phone firmware is not matched within the table.

Private key updates

You rarely need to perform a private key update. Private key updates are required if a key has been compromised or as part of standard security policy to limit the period an individual key is in use. After a private key update, all

IP Phones must be transitioned to the new key fingerprint within a bounded period of time. Within five minutes of a key update, the SMC automatically updates the private key for IP Phones currently connected to the device. However, additional IP Phones that may be offline at the time of the transition, this update occurs at a later time, after they re-establish connectivity.

Because of the possibility of delayed private key updating, Nortel recommends that the primary and secondary keys co-exist for the length of time equal to the maximum session timeout plus the master key timeout. The phones using session caching do not touch the key when they reconnect and, therefore, are not updated). They will, however, have their fingerprints replaced when they change their session keys.

Licensing

The SMC requires a license to support the total number of Secure UNIStim users. Without a license key, the SMC supports 50 Secure UNIStim users. However, you can purchase licenses for 250, 500, 1000, 3000, and 5000 simultaneous users. There is no license limitation on non-secure UNIStim users or other traffic that traverses the SMC.

WARNING

When the license is exceeded and the policy does not require security, additional IP Phones are allowed through insecurely. If the policy requires security, the license prevents any additional phones from connecting insecurely.

Using the MAC address of the first Ethernet port, licensing is defined separately for each SMC. In a HA configuration, a license is required for each SMC. Licenses can be additive; if the same Mac address is specified when the keycode is supplied, additional licenses can be added to an existing system.

You can apply purchased licenses to the system using either the BBI or the CLI:

- In the BBI, navigate to the **Cluster > Host > License** page.

- In the CLI, type **`/cfg/sys/cluster/host <n>/license, where <n>`** is the host number.

Troubleshooting

Current servers

View the number of primary and secondary servers on the System page or at the **Administration > Monitor > UNIStim Security > Servers** page in the Web UI.

Current clients

View the number of secure and insecure UNIStim sessions on the System page or at the **Administration > Monitor > UNIStim Security > Servers** page. Note that clients that are not associated with a proxied server and that pass through the firewall insecurely using a firewall rule are not included in these counts.

Statistics

View the UNIStim proxy statistics at the **Statistics > UNIStim Proxy** page.

IMPORTANT!

Secure UNIStim statistics only count clients that connect to proxied servers. That is, those that are actively served by the Secure UNIStim transparent proxy. Clients to non-proxied servers communicate directly through the firewall and are not counted in these statistics.

Scenarios

This section details selected Secure UNIStim deployment scenarios.

Disabling Secure UNIStim

When you disable Secure UNIStim, all currently proxied sessions are reset and their calls are dropped. The IP Phones reconnect to the Signaling Server

using insecure UNIStim, provided the action byte is not set to 6 in the IP Phone configuration or through DHCP.

IMPORTANT!

IP Phones that are already running Secure UNIStim have a key fingerprint installed on them. This prevents them from connecting securely with another SMC that doesn't support the same private key, either as a primary or a secondary key.

Reenabling Secure UNIStim

When Secure UNIStim is turned on again in an installation that is already primed with IP Phone fingerprints, the IP Phones reconnect using the fingerprints already installed on the IP Phones.

Client policy and client firmware policy issues

The client subnet consists of IP Phones with and without the capabilities to run secure UNIStim. The IP Phone 2050 is an example of an IP Phone that does not support secure UNIStim.

SMC provides options to configure IP Phone firmware policies based on the IP Phone firmware version and client policies based on client IP address and subnet information. These policies impact IP Phone connectivity in the following ways:

- allow or deny a IP Phone non-secure register request
- force an IP Phone to upgrade from non-secure to secure UNIStim
- allow or deny IP Phone fingerprint update based on client address information
- allow or deny IP Phone fingerprint update based on IP Phone firmware version
- allow or deny IP Phone session caching based on client address information

- allow or deny IP Phone session caching based on IP Phone firmware version

This section provides specific examples to clarify how to apply these policies to serve your specific needs.

Example 1

In this example, use the default policy to control the access so that IP Phones with secure capability connect in secure mode and IP Phones without secure capability connect in insecure mode.

Policy setting:
upgrade = y
Security = n

Example 2

In this example, use the default policy to control the access so that IP Phones with secure capability connect in secure mode and IP Phones without secure capability get rejected.

Policy setting:
upgrade = y
Security = y

Example 3

The client subnet consists of IP Phones running the newer firmware as well as the older firmware. Older firmware, such as the 0602B76, sometimes enables session caching and causes the IP Phone to lose the Terminal Number (TN)/Directory Number (DN) information. To optimize performance, all IP Phones on the client subnet should utilize the session caching feature. Disable session caching on the older firmware. You can achieve this goal with the following policies:

Policy setting:
upgrade = y
Security = (y or n)

cache = y

Add a firmware policy for 0602B75:
cache = deny

IMPORTANT!

Once firmware checking is enabled, you must ensure that all firmware versions that need to run secure UNIStim are present in the firmware database. The SMC assumes that if the firmware is not in the database, it does not have secure UNIStim capabilities.

Maintenance

Contents

This chapter contains information about the following topics:

Introduction

This chapter contains information about how to access system management features on the SMC. Management access is required for collecting system information, configuring system parameters beyond initial setup, establishing security policies, and monitoring policy effectiveness.

Management tools

The SMC provides the following system management tools:

- Command Line Interface (CLI)

  The CLI offers a text-based menu system for collecting system information and configuring system parameters. Use of the CLI is required for initial setup of the system. You can access the CLI accessed locally at the SMC or remotely through Telnet or Secure Shell (SSH)

after access is granted. See "Defining the remote access list" on page 109.

- Web User Interface (UI)

  After initial setup is complete, enable Web UI access through the CLI. Using the Web UI, you can manage the SMC through a Web browser. The Web UI provides a richly featured graphical user interface that enables routine configuration and data collection.

Users and passwords

Access to system functions is controlled through the use of unique usernames and passwords. Once you are connected to the system through the local console, Telnet, SSH, or Web browser, you are prompted to enter a password. To enable better administration and user accountability, four levels of user access are implemented on the SMC. The default usernames and password for each access level are listed in Table 14. Usernames and passwords are case sensitive.

Note: Nortel recommends that you change all the default passwords after initial configuration and as regularly as required under your network security policies.

Table 14
User access levels

Username	Password	Description and Tasks Performed
oper	oper	The operator login is available through the CLI and Web UI. The operator has no direct responsibility for administration. The operator can view all configuration information and operating statistics, but cannot make any configuration changes.
admin	admin	The administrator login is available through the CLI and Web UI. The administrator has complete access to all menus, information, and configuration commands on the system, including the ability to add users and change passwords.

Table 14
User access levels

Username	Password	Description and Tasks Performed
boot	ForgetMe	The boot login is available only through a local console terminal. The boot user can reinstall the SMC software. To ensure that one avenue of access is always available in case all passwords are changed and lost, the boot user password cannot be changed.
root	ForgetMe	The root login is available only through a local console terminal. The root user has complete internal access to the operating system and software. Root access is NOT RECOMMENDED unless under the direction of Nortel support personnel.

CAUTION — Service Interruption
The root login on this system is only intended for debugging and emergency repair, typically under the direction of support personnel. All modifications to the system, including configuration changes of any kind, must be made through the CLI available for the admin login. Modifications made using the root login can cause serious malfunction of the system, and also can be reversed by the system at any time.

SMC software upgrades

The SMC software can be upgraded using the following methods:

- Package upgrade: Using the CLI or Web UI (preferred), a single file is pushed to the SMC, unpacked, and then activated by an automated reboot. This is the recommended upgrade process. The package upgrade retains the current SMC configuration. The SMC can hold two package files on the system, so you can revert back to the original if required.
- Image upgrade: Using the CLI, a single file is loaded from CD-ROM (ISO install CD) or through FTP/TFTP to the SMC. The file is then unpacked and activated. This upgrade process DOES NOT retain the current configuration, so the configuration must be saved prior to the upgrade. Use this upgrade when there is concern that the SMC application software is corrupt but the Operating System is intact.
- ISO install CD: Using the CLI, the SMC is booted with the Install CD-ROM. The hard drive on the SMC is reformatted and all software is reinstalled. The configuration must be saved prior to the ISO install because the configuration is lost during the install. This process is used to restore the SMC to the factory default state.

The upgrade files are provided on the Nortel web site. The package files have a .PKG extension, and the ISO Install CD has an .ISO extension.

IMPORTANT!

Nortel recommends that you perform software upgrades during a maintenance window since the upgrade can impact service.

Upgrading SMC software

Prior to upgrading the SMC software, save the configuration and the keys. See "Saving and restoring the SMC configuration" on page 115.

IMPORTANT!

Nortel recommends that you perform software upgrades during a maintenance window since the upgrade can impact service.

Upgrading SMC software using a package upgrade (Web UI)

Procedure 43
Upgrading SMC software using a package upgrade (Web UI)

1 Using a Web browser, enter the URL to the Web management interface.

The SMC login prompt appears.

2 Enter Web UI admin account and password.

3 On the left hand side of the page, click **Operation > ImageUpdate**.

Two options are displayed: Packages or Patches.

4 Click **Packages**.

A screen appears listing the Installed Packages and providing an option to upload the new package.

5 Click **Browse** to locate the package you wish to upload to SMC.

Note: The package file is already downloaded from the Nortel Web site and saved onto the PC. Package files end with the extension .PKG.

6 Select the package to upload.

7 Click **Submit**.

Note: The upload time depends upon the speed of the Internet connection. Slow connections can take many minutes.

Once the package is uploaded, the Installed Packages section of the page shows the package with a status of "Unpacked". Two options are displayed in the Action column: Activate and Delete.

8 Click **Activate**.

A confirmation dialog appears and displays the following message: Are you sure you want to activate this image?

WARNING

Activating a Package requires the SMC to reboot itself.

9 Click **Ok**.

The page refreshes and the package is marked as old.

10 Click **Activate** again.

The SMC installs the package and then reboots. The reboot can take up to 5 minutes to complete.

11 Log back on with the admin username and password.

12 Click **Operations > Image Update > Package** to verify that the desired package is activated.

End of Procedure

Result: The new package has a status of *permanent* indicating that it is now the active version. The pervious package has a status of old with an Activate button in the Actions column of the page. The Activate button provides the option to revert to the previous package, if needed.

Upgrading SMC software using a package upgrade (CLI)

To install a package upgrade on the SMC, you need the following:

- CLI access to the SMC host through a local console terminal or a remote Telnet or SSH connection.
- The IP address of the FTP/TFTP/SCP/SFTP server that is operating on the network and has been loaded with the package file to load onto the SMC.
- This process assumes that FTP, TFTP, or both are enabled on the SMC. See Procedure 28 on page 116 for information.

Telnet and SSH connections are disabled by default; therefore, you must enable them after you set up the SMC. For more information about enabling Telnet and SSH connections, see “The Command Line Interface (CLI)” on page 187.

Procedure 44
Upgrading SMC software using a package upgrade (CLI)

1 Start a console terminal.

2 Press <Enter> on the console terminal to establish the connection.

Result: The SMC login prompt appears.

3 Log on with the admin user and password.

4 Enter **`cur`** to verify the current versions of the software.

5 Choose one of the following:

If	Then
FTP or TFTP download	**1** Enter **`/boot/software/download`**. **2** Enter **`ftp`**. **3** Enter the IP address of server. **4** Enter the filename on server. **Result**: The software is downloaded onto the SMC.
CD-ROM download	**1** Enter **`/boot/software/cdrom`**. **2** Insert the installation CD-ROM. ***Note:*** For this command to be accepted, the CD-ROM tray must be closed. **3** Press <Enter>. **Result**: The software is downloaded onto the SMC.

4 Enter **`cur`** to verify the current versions of the software.

5 Verify that the version you downloaded has a status of unpacked.

The software versions are marked with one out of four possible status values. The meaning of each status value is described in Table 15.

Table 15
Software status values

Status	Meaning
unpacked	The software upgrade package is downloaded and automatically decompressed.
current	A software version previously marked as old or unpacked is activated. After the system performs the necessary health checks, the current status changes to permanent.
permanent	The software is operational and can survive a reboot of the system.
old	The software version is not currently operational.

After the upgrade is loaded, you must activate the software. The process is slightly different for a stand-alone configuration. See “Activating the software” on page 172.

End of Procedure

Activating the software

The SMC can hold up to two versions of the same major software release simultaneously. To view the current software status, use the **`/boot/software/cur`** command.

When a new version of the software is downloaded to the SMC, the software package is automatically decompressed and marked as unpacked. After you activate the unpacked software version, which causes the SMC to reboot, the software version is marked as permanent. The software version previously marked as permanent is then marked as old.

Procedure 45
Activating the software for a stand-alone upgrade

For this procedure, it is assumed that you already logged on and loaded the SMC software.

1 Enter **`/boot/software/cur`** to inspect the status of the software package.

2 Enter **`/boot/software/activate n.n.n.n`**, where n.n.n.n is the software version, to activate the new software package.

3 Enter **`y`** to confirm you want to activate the software.

4 Log in with the admin user and password.

Wait for the SMC to restart and initialize all system components. When the SMC restarts, wait a few more minutes. Do not disturb the system until it responds with the Login prompt and then wait two more minutes for the SMC to be reinitialized.

5 Enter **`/info/clu`** to check that the SMC is running.

6 Log on to the SMC.

7 Enter **`/boot/software/cur`** to check the software status.

The software version that was previously marked as permanent is now marked as old. The new software version is marked as permanent.

End of Procedure

Procedure 46
Activating the software for a cluster upgrade

For this procedure, it is assumed that you already logged on and loaded the SMC software.

1 Enter **`/info/summary`**.

2 Determine which SMC holds the cluster MIP.

The SMC with the asterisk (*) in the cluster MIP column holds the cluster MIP.

3 Log on to the SMC with the cluster MIP using the admin account through the console or Telnet/SSH.

4 Enter **`/cfg/sys/accesslist/list`** to verify that an access list exists that includes all addresses on the management interface. If this entry does not exist, add it.

5 Enter **`/boot/software/cur`** to check the current version of the software.

6 Enter **`/boot/software/activate n.n.n.n`**, where n.n.n.n is the software version, to activate the new software package.

7 Enter **`y`** to confirm you want to activate the software.

Wait for the SMC to restart and initialize all system components. When the SMC restarts, wait a few more minutes. Do not disturb the system until it responds with the Login prompt and then wait two more minutes for the SMC to be reinitialized.

The software version that was previously marked as permanent is now marked as old. The new software version is marked as permanent.

8 Wait for a few minutes for the SMCs to initialize all system components.

9 Enter **`/info/net/vrrp/status`** to verify VRRP status.

End of Procedure

Result: When the upgrade is completed, the configuration for at least one network interface must be added so the configuration can be downloaded using FTP/TFTP.

Reinstalling the software

Reinstalling the software is seldom required except after a serious malfunction. To reinstall software on the SMC, you must connect directly to the SMC serial port and log on as the boot user with the ForgetMe password. When the reinstallation is performed, the new SMC is reset to factory default configuration. All previous configuration data and software is erased, including old software image versions or upgrade packages.

A reinstallation erases all configuration data, which includes installed keys, network settings, and certificates. Nortel recommends that you save all configuration data to a file on a TFTP/FTP/SCP/SFTP server using the ptcfg command. See “Saving and restoring the SMC configuration” on page 115.

Two methods are available for reinstalling software on the SMC:

- using the .ISO image of the software. See Procedure 47 on page 175.

- using the .IMG image of the software. See Procedure 48 on page 176.

Procedure 47
Reinstalling the software using the .ISO image

Nortel recommends this method to copy the .ISO version of the software on a CD-ROM and boot from it. This reinstall removes the current configuration and reimages the SMC.

1 Burn the .ISO file to a CD-ROM as an .ISO image.

2 Make sure that the configuration and the keys are backed up. See "Saving and restoring the SMC configuration" on page 115.

3 Insert the .ISO Image CD-ROM into the SMC.

4 Restart the SMC to cause it to boot from the CD-ROM.

If the CD-ROM is correctly burned and inserted, you will see the following message: `Loading OS from CDROM`.

5 When prompted, log on to the console as the root user. No password is required.

IMPORTANT!

If the SMC booted from the CD-ROM, the following prompt is displayed: `[root@localhost root]#`. If the prompt is similar to `[root@a47-11-102-243 root]#`, the SMC did not boot from the CD-ROM.

6 Enter **`install-smc SMC-2450`**

7 Wait 15 minutes for the installation script to finish.

If the SMC doesn't reboot automatically, take the software CD-ROM out and reboot the SMC.

8 Log on with the admin user and password.

9 Proceed with Procedure 18 on page 102 to configuration the SMC.

Note: As a minimum, the management and intranet interfaces must be configured so that FTP/TFTP can be used to retrieve and restore the configuration from the server.

End of Procedure

Procedure 48
Reinstall the software using the .IMG image

This method installs the IMG version of the software using TFTP or FTP. This reinstall overwrites the current configuration. In this procedure, you instruct the SMC to use a specific network interface and use a specific IP address to pull the Image file from the TFTP or FTP server.

To reinstall the software using FTP/SCP/SFTP, you need the following:

- Access to the SMC through a direct connection to its serial port. You cannot use remote Telnet or SSH connections for reinstalling software.
- An .IMG file loaded on a FTP/SCP/SFTP server on the network.
- The host name or IP address of the FTP/SCP/SFTP server.
- The name of the .IMG file.
- This process assumes that FTP and TFTP are enabled on the SMC. See Procedure 28 on page 116.

Note: You can press **Ctrl + C** to exit the reinstall process.

1. Back up the configuration and keys as required. See Procedure 27 on page 115.
2. Connect to the SMC through the serial port.
3. Log on as the boot user with the default password is ForgetMe.
4. Enter `y` to continue.
5. Choose one of the following:
   a. Select a network port.

      The interface mappings are as follows:

      eth0 = motherboard port (SMC Port 1)
      eth1 = motherboard port (SMC Port 2)
      eth2 = NIC Card port 4 (SMC Port 3)
      eth3 = NIC Card port 3 (SMC Port 4)
      eth4 = NIC Card port 2 (SMC Port 5)
      eth5 = NIC Card port 1 (SMC Port 6)

   b. Press <Enter> if the default is correct.
6. Enter the IP address to be used by the network interface.
7. Enter the network subnet mask.

8 Enter the gateway IP address.

9 Choose one of the following:

a. Enter **`t`** to select TFTP.

b. Enter **`f`** to select FTP.

10 Enter the TFTP server IP address.

11 Enter the filename of boot image.

12 Log on as the boot user.

13 Enter the password.

After the new boot image is installed, the SMC reboots and you can log on again when the login prompt appears.

14 Enter **`/cfg/gtcfg`** to restore the configuration from the TFTP server.

15 Reboot the SMC to apply the restored configuration file.

End of Procedure

Resetting the SMC to factory defaults

WARNING
Resetting the SMC to factory defaults halts all current operations on the SMC.

Procedure 49
Resetting the SMC to factory defaults

When you configure the SMC for the first time, the unit is already set to factory defaults; therefore, you can skip this procedure. However, if you wish to override the previous configuration, perform the following steps:

1 Do one of the following:

- Reset a standalone SMC installation to factory default.
  - CLI: **`/cfg/sys/cluster/host 1/delete`**

— Web UI: **Operation > SMC Host(s)**
Select the host you want to delete and then click **Delete**.

WARNING

Deleting the host to which the Web UI is connecting causes the browser to lose connectivity.

- Reset a High Availability SMC installation to factory default.

  i. First determine which machine one is currently logged in to

  If one SMC is using one of the real IPs, the address is the Real IP address. If one SMC is using the MIP, you can determine which SMC owns the MIP in the following manner:

  — CLI: **`/info/summary`**

  — Web UI: **System page**

WARNING

The delete command fails if HA is enabled. Disable HA before deleting the SMC.

- CLI: **`/cfg/net/vrrp/ha`**
- Web UI: **Network > VRRP > High Availability**

  ii. Delete the machine not currently logged on (connectivity is not lost).

  — CLI: /cfg/sys/cluster/host <n>/delete

  — Web UI: Operation -> SMC Hosts -> Delete

WARNING

When the second machine is deleted, Web UI / CLI access is lost; connectivity is only allowed through the Console

2 Restart the SMCs.

3 Perform the initial setup procedure. See “Configuring the initial SMC” on page 102.

End of Procedure

VRRP overview

The Virtual Router Redundancy Protocol (VRRP) eliminates single point of failure by dynamically assigning responsibility for a virtual router to one of the physical routers on a LAN. VRRP provides a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

IMPORTANT!

VRRP is defined by RFC 2338; however, VRRP on the SMC is a custom implementation that deviates from RFC 2338 in the following ways:

- To verify a host is down before failover, VRRP uses its own checking mechanism.
- To limit the number of failovers when a device goes down and comes back up, VRRP does not support preferred master.

The SMC does not work with Spanning Tree Protocol (STP) because STP interferes with VRRP. When STP is enabled, the SMC host with the highest IP address always become master. This leads to two failovers if the master SMC fails: the first failover occurs when the master fails and the second failover occurs when it restarts. This double failover is due to a race condition between the VRRP advertisements and the reconverging STP. The rebooted machine may not receive the advertisements from the new master prior to its becoming master itself, thereby leading to a master-master election process.

Note 1: If any of the six SMC ports are connected to a Layer 2 switch, the master election process occurs when STP-enabled Layer 2 switch link is failed over. A single port pair behaving as previously described invokes the master election process behavior.

Note 2: In VRRP election, the only relevant IP address is the cluster MIP address.

The SMC that assumes the virtual router IP addresses is called the active master, and it forwards packets intended for these IP addresses. If the active master becomes unavailable, VRRP provides dynamic failover in the forwarding responsibility to a redundant VRRP router. This dynamic failover enables the end-hosts to use the virtual router IP addresses as the default first hop router, regardless of which VRRP router is active.

Two SMCs in a High Availability configuration communicate with each other using *VRRP packets*. The purpose of the VRRP packet is to communicate the state of the active SMC. VRRP packets are encapsulated in IP packets that are sent to the multicast group address (224.0.0.18) assigned to VRRP.

High Availability configuration

A cluster is created when a second SMC is added to the first SMC. Only two SMCs can reside in a cluster. The general procedure for joining the SMCs is presented in “Installing the redundant SMC” on page 118.

Clustered SMCs act as virtual routers in a redundant relationship using VRRP.

IMPORTANT!

In an active-standby (HA) configuration, only one SMC passes traffic, while the redundant SMC is a dedicated backup.

In all cases, the assumption of the active role is managed by the VRRP election process. Past the initialization stage, the role of active master is independent of the default condition. See “Active master determination” on page 180.

Active master determination

VRRP ensures that one virtual router or the other assumes the role of active master. VRRP election, the process that determines the active master, occurs during initialization (that is, when VRRP is enabled for the HA cluster) or during SMC start-up. VRRP failover occurs when the backup fails to receive advertisement packets at preset intervals from each interface on the active

master. Both processes ensure that only one SMC is active at a time and that the active SMC can communicate on the LAN. VRRP election and VRRP failover are described on page 181.

VRRP election

At start-up, the virtual routers on both SMCs start in the backup state and then wait for advertisement packets. Only active masters broadcast advertisement packets. When no advertisement packets are received, each virtual router assumes the active master role and both virtual routers begin broadcasting advertisement packets. After the virtual router detects advertisement packets from the other SMC, the virtual router with the lower IP address (default backup) reverts to backup, leaving the virtual router with the higher IP address (default master) as the active master.

The active master continuously broadcasts advertisement packets at regular intervals as defined by the advertisement interval (adint) value. If advertisement packets are not received within the advertisement interval, VRRP failover begins on the backup.

Reasons why advertisement packets do not reach the backup include:

- the active link is down
- the port is down
- high traffic spreads advertisement packets beyond the specified adint interval
- a device on the virtual router LAN blocks the advertisement packets or Address Resolution Protocol (ARP) traffic

VRRP failover

VRRP failover occurs when the backup fails to receive advertisement packets at preset intervals from each interface on the active master.

If VRRP multicast advertisement packets to group address 224.0.0.18 are not received on any backup virtual router, each backup virtual router sends four ARP requests (one per second) to the active master virtual router IP addresses. This gives the active master ample opportunity to respond,

enabling the backup virtual routers to confirm that it is down before going on to the next step:

- If ARP replies from the active master are not received, failover occurs.
- If ARP replies from the active master are received, no failover occurs.

  Note: If VRRP multicast advertisement packets are not received on any backup router, the reason might be that the traffic on the active master is too heavy for it to send advertisement packets within the advertisement interval. If you believe this is the case, increase the advertisement interval value.

When a virtual router comes up from the fault state, it sends ARP requests for an active master. If the virtual router receives an ARP response, the virtual router assumes the role of backup. The backup continues sending ARP messages to the virtual router until it does not receive a response and then initiates the failover process.

VRRP failover based on links

Link failures decrement the internal priority value that VRRP maintains for both SMCs. A link failure is defined as a loss of link at the VRRP interface. At initialization, VRRP sets the priority value to 100 for both SMCs. When a physical link fails, VRRP reduces the priority value for that SMC by two. If that causes the SMC's priority value to fall below that of the other SMC, failover occurs.

When the link is restored, the priority value for that SMC is increased by two. This can cause both SMCs to have the same priority values. Nevertheless, the cluster status does not change until a link failure occurs on the backup and this causes VRRP to reduce its priority value by two and trigger a failover.

MAC address mapping

The active master uses its virtual router ID (vrid) to set a unique virtual router MAC address according to this formula: 0x00005E0001<vrid>. This is the address that the active master returns in response to end-host ARP requests and proxy ARP requests. Gratuitous ARP (GARP) messages also contain the active master's virtual router MAC address. Meanwhile, the backup retains its physical MAC address.

When the active master becomes the backup, it overwrites its virtual router MAC address with its physical MAC address. At the same time, the newly active master overwrites its physical MAC address with its unique virtual router MAC address.

> ***Note:*** In practice, GARP messaging is usually the mechanism that informs switches and routers of MAC address changes.

VRRP router parameters

You can define VRRP router parameters globally using either the CLI or the Web UI. You can use the following parameters to configure VRRP:

- Active-Standby
- Advertisement interval
- Gratuitous ARP (GARP)
- VRRP interface
- Advanced failover check

Active-Standby

The active-standby parameter enables Active-Standby, which is also referred to as HA. You can apply Active-Standby only when there are two SMCs in the cluster.

Advertisement interval

The advertisement interval parameter sets the interval in seconds between advertisement messages, which are multicast to 224.0.0.18 from the active master's subaddress. See "VRRP interface" on page 184. If the backup does not receive advertisement messages at the specified interval, the VRRP failover process begins.

It can be necessary to increase the advertisement interval during high traffic periods that prevent the active SMC from issuing advertisement messages at the specified interval. Increasing the advertisement interval lowers the chance for unnecessary disruption of packet forwarding, but increases the length of service disruption in the event that the active master fails.

Gratuitous ARP (GARP)

After the backup detects a failure in the active master, the backup immediately flashes a Gratuitous ARP (GARP) message to the end-hosts on the virtual router interface.

The GARP, an unsolicited ARP response, forces end-hosts to update their ARP caches with the new MAC address and IP address mapping. Then the backup delays a period of time defined by the GARP delay value before sending continuous GARP messages at intervals defined by the Gratuitous Broadcast value. The GARP message shortens the time it takes an SMC to discover a lost backup. Continuous GARP messages prevent end-hosts from aging out their ARP entries for the virtual router.

Increasing the Gratuitous Broadcast value cuts down on the GARP traffic, but lengthens the interval between end-host ARP cache updates.

VRRP interface

Define the Virtual router network interface parameters per virtual router at the VRRP Interface Menu. Before you configure the virtual router network interface parameters, you must first configure the network interface IP parameters at the Interface Menu. Each virtual router interface requires the following parameters:

- a common virtual router IP address
- a common virtual router ID (vrid)
- two subaddresses (one representing each SMC host)
- a common port on each SMC

Real router IP addresses

The real router IP addresses are assigned to the physical SMC.

The IP addresses (ip1 and ip2) you enter at the Interface Menu become the real router IP addresses. You can also enter other real interface parameters, including the port.

Virtual router IP addresses

The virtual router IP addresses is a floating IP address is associated with the master SMC.

Define the vrid and virtual router IP addresses at the VRRP Interface menu on the same interface as the virtual router interface. The virtual router IP address and the subaddresses must be unique, but all three IP addresses must belong to the same subnet.

Advanced failover check

If Advanced Failover Check (AFC) is enabled, the system sends an ARP message before initiating a failover caused by missed VRRP advertisements.

The Command Line Interface (CLI)

Contents

This chapter contains information about the following topics:

Introduction

The Command Line Interface (CLI) is the most direct method for viewing information about the Secure Multimedia Controller (SMC). In addition, you can use the CLI for performing all levels of system configuration.

You can view the text-based CLI using a basic terminal. The CLI commands are grouped into a series of menus and submenus. Each menu displays a list of commands and/or submenus, along with a summary of what each command does. Below each menu is a prompt in which you can enter any command appropriate to the current menu.

This chapter describes how to access the CLI locally through any SMC serial port, or remotely using a Telnet or Secure Shell (SSH) client. It also provides a list of commands and shortcuts that are commonly available from all the menus within the CLI.

> ***Note:*** Before you can use the CLI, a minimum configuration must be entered as described in “Configuring the initial SMC” on page 102.

Accessing the CLI

Using the local serial port

Any SMC serial port provides direct local access for managing the SMC. For details on attaching a console terminal to the serial port and establishing a connection, see “Hardware installation” on page 59.

After the connection is initiated, you are prompted to log on and enter a valid password. For more information about different access levels and initial passwords, see “Users and passwords” on page 166. When the login is validated, the Main Menu of the CLI appears.

Using remote access

Using Telnet

Using a Telnet connection, you can manage the SMC from any workstation connected to the network. Telnet access provides the same management options as those available through the local serial port.

By default, Telnet access is disabled and all remote access is restricted. Depending on the severity of the security policy, you can enable Telnet and permit remote access to one or more trusted client stations. See “Defining the remote access list” on page 109.

> ***Note:*** Telnet is not a secure protocol. All data, including the password, between a Telnet client and the SMC is unencrypted and unauthenticated. If secure remote access is required, consider using Secure Shell (SSH). See “Using Secure Shell (SSH)” on page 189.

Enabling Telnet access

For security purposes, Telnet is initially disabled. Before Telnet access is possible, you must first perform some configuration using the serial port.

Procedure 50
Enabling Telnet using the CLI

1 Start a console terminal.

2 Press <Enter> on the console terminal to establish the connection.

The SMC login prompt appears.

3 Enter the admin username and password.

4 Enable Telnet.

   a. Enter **`/cfg/sys/adm/telnet/ena`**

   b. Enter **`apply`**

5 Use the access list to permit remote access to trusted clients. See “Defining the remote access list” on page 109.

   Note: If you already configured the access list for SSH or the Web UI, there is no need to perform step 5.

End of Procedure

Starting the Telnet session

Remote Telnet access requires a workstation with Telnet client software.

To establish a Telnet session, run the Telnet client software and issue the Telnet command on the workstation:

```
telnet <host IP address>
```

Connect to the SMC host IP address

Once the Telnet session is initiated, you are prompted to log on and enter a valid password. See “Users and passwords” on page 166.

When the login is validated, the Main Menu of the CLI appears.

Using Secure Shell (SSH)

Using an SSH connection, you can manage the SMC from any workstation connected to the network. SSH access provides the same management options as those available through the local serial port.

SSH access provides the following security benefits:

- server host authentication
- encryption of management messages
- encryption of passwords for user authentication

By default, SSH access is disabled and all remote access is restricted. Depending on the severity of the security policy, you may enable SSH and permit remote access to one or more trusted client stations. See "Defining the remote access list" on page 109.

Enabling Telnet or SSH using the Web UI

Procedure 51
Enabling Telnet or SSH using the Web UI

1. Using a Web browser, access the Web UI.
2. Log on using the administrator account and password.
3. Click **Administration > Telnet-SSH**.

A page is displayed that shows the state of Telnet and SSH access. Make sure the access method you wish to use is enabled.

4. If Telnet or SSH is not enabled, perform the following tasks:
   - Set the SSH state to **Enabled** and then click **Update**.
   - Set the Telnet state to **Enabled** and then click **Update**.
5. Click **Apply** in upper right hand part of the page.

The Apply Pending Configuration Changes page is displayed.

6. Select **Apply Changes**.
7. Click **Submit**.

End of Procedure

You can log on to SMC using Telnet or SSH from any workstation whose IP address is included in the access list.

Enabling SSH

Before SSH access is possible, you must first configure the SMC to allow SSH access.

Procedure 52
Enabling SSH using the CLI

1 Start a console terminal.

2 Press <Enter> on the console terminal to establish the connection.

The SMC login prompt appears.

3 Enter **`admin`** for the default login name.

4 Enter **`admin`** for the default password.

5 Check that the SMCs are configured with proper IP addresses.

6 Enable SSH access.

   a. Enter **`/cfg/sys/adm/ssh/ena`**.

   b. Enter **`apply`**.

7 Generate new SSH keys.

   During the initial setup of the SMC, Nortel recommends that you select the option to generate new SSH host keys. This is required to maintain a high level of security when connecting to the SMC using an SSH client. If you fear that the SSH host keys are compromised, or at any time the security policy dictates, you can create new host keys.

   When reconnecting to the SMC after generating new host keys, the SSH client displays a warning that the host identification (or host keys) is changed.

   a. Enter **`/cfg/sys/adm/ssh/gensshkey`**.

   b. Enter **`apply`**.

8 Use the access list to permit remote access to trusted clients. See “Defining the remote access list” on page 109.

   Note: By default, administration access is only allowed through the management subnet. You need to add entries to the access list and then enable the Web UI, SSH, and Telnet. Users can access management only through the host IP address or the Master IP.

To access management capabilities using the Intranet IP address and the Intranet subnet, see Procedure 19 on page 106.

Starting the SSH session

Remote SSH access requires a workstation with SSH client software, such as TTY.

Note: You cannot log on as boot or root using SSH.

After the SSH session is initiated, you are prompted to log on and enter a valid password. See "Users and passwords" on page 166. When the login is validated, the Main Menu of the CLI appears.

Using the CLI

Basic operation

Using the CLI, SMC administration is performed in the following manner:

1. From a series of menu and submenu items, modify parameters to create the desired configuration.
2. Use the global **`cur`** command to view the current settings for the commands in the current menu.
3. Use the global **`diff`** command to view pending changes before they are applied.

   Most changes are considered pending and are not immediately put into effect or permanently saved. Only a few types of changes, such as changes to users and passwords, take effect when entered.

4. Use the global **`apply`** command to save changes and make them take effect.
5. Choose one of the following:

a. Use the global **revert** command to clear all pending changes and then continue the configuration session.

b. Use the global **exit** command to logout from the system. Closing the remote session also discards pending changes, though Nortel recommends that you close the remote session using the **exit** command.

The Main Menu

After initial system setup is complete and the user performs a successful connection and login, the Main Menu of the CLI appears.

Idle time-out

By default, the system disconnects the CLI session after 5 minutes of inactivity. This function is controlled by the idle time-out parameter as shown in the following command: **`>> # /cfg/sys/adm/idle <time-out period>`** where the time-out period is specified as an integer from 300 to 3600 seconds. Or you can specify time-out in minutes, from 5 minutes (5m) to 60 minutes (60m).

Multiple administration sessions

It is possible to have more than one CLI or Web UI administrator session open at a time. Although each concurrent administrator session is independent, the saved changes affect all users when configuration changes are saved. However, if multiple CLI or Web UI administrators apply changes to the same set of parameters concurrently, the latest applied changes take precedence.

Global commands

Some basic commands are recognized throughout the entire menu hierarchy. These commands are useful for obtaining online help, navigating through menus, and for applying and saving configuration changes.

Table 16
Global CLI commands

Command	Description
help <command>	Provides more information about a specific command on the current menu. When used without the command parameter, provides a summary of the global commands.
.	Redisplays the current menu.
.. or up	Goes up one level in the menu structure.
/	If placed at the beginning of a command, goes to the Main Menu. Otherwise, separates multiple commands placed on the same line.
apply	Applies and saves pending configuration changes.
diff	Shows any pending configuration changes.
exit	Exits from the CLI and logs out.
cur	Displays the settings for the commands on the current menu. The output of the **`cur`** command is for viewing only. You cannot save and restore it later. If you wish to save the configuration for restoration later on, use the **`dump`** or **`ptcfg`** commands.
validate	Validates the configuration.
security	Displays the security status of the SMC.
lines <n>	Sets the number of lines that display on the screen. The default value is 24 lines.

Table 16
Global CLI commands

Command	Description
nslookup <host name> <IP address>	Finds the IP address or host name of a network device. To use this command, you must configure the SMC to use a DNS server. If you did not specify a DNS server during the initial setup procedure, you can add a DNS server at any time by using the **`/cfg/sys/dns/add`** command.
paste	Sets a password for restoring a saved configuration dump file that includes encrypted private keys.
ping <address> <tries> <delay>	Verifies station-to-station connectivity across the network.
pwd	Displays the command path used to reach the current menu.
revert	Cancels all pending configuration changes.
traceroute <address> <max-hops> <delay>	Identifies the route used for station-to-station connectivity across the network.
verbose <n>	Sets the level of information displayed on the screen: 0 = Quiet: Nothing appears except errors—not even prompts. 1 = Normal: Prompts and requested output are shown, but no menus. 2 = Verbose: Everything is shown.

Command Line history and editing

Using the CLI history and editing commands, you can retrieve and modify previously entered commands with just a few keystrokes.

Table 17
Command Line history and editing options

Command	Description
history	Displays a numbered list of the last 10 previously entered commands.
!!	Repeats the last entered command.
!<n>	Repeats the nth command shown on the history list.
<Ctrl-p> or the up arrow key	Recalls the previous command from the history list. You can use this command multiple times to navigate backward through the last 10 commands.
<Ctrl-n> or the down arrow key.	Recalls the next command from the history list. You can use this command multiple times to navigate forward through the last 10 commands.
<Ctrl-a>	Moves the cursor to the beginning of command line.
<Ctrl-e>	Moves cursor to the end of the command line.
<Ctrl-b> or the left arrow key	Moves the cursor back one position to the left.
<Ctrl-f> or the right arrow key	Moves the cursor forward one position to the right.
<Backspace> or the Delete key	Erases one character to the left of the cursor position.
<Ctrl-d>	Deletes one character at the cursor position.
<Ctrl-k>	Erases all characters from the cursor position to the end of the command line.
<Ctrl-l>	Redraws the screen.

Table 17
Command Line history and editing options

Command	Description
<Ctrl-u>	Clears the entire line.
Other keys	Inserts new characters at the cursor position.

Command line shortcuts

Command stacking

As a shortcut, you can stack commands by typing multiple commands on a single line separated by forward slashes (/). You can connect as many commands as required to access the menu option that you want. For example, the command stack to access Access List menu from the Main# prompt is as follows:

```
>> Main# cfg/sys/accesslist
```

Command abbreviation

To abbreviate commands, enter the first characters that distinguish the command from the others in the same menu or submenu. For example, you can enter the preceding command as follows:

```
>> Main# c/s/acc
```

Tab completion

Enter the first letter of a command at any menu prompt and press <Tab> to display all commands in that menu beginning with the letter you typed. You can further refine the list of commands or options displayed by typing additional letters. If only one command matches the letters when <Tab> is pressed, that command is supplied on the command line. You can then execute the command by pressing <Enter>. If the <Tab> key is pressed without any input on the command line, the currently active menu appears.

RADIUS authentication

SMC 2450 enables you to log on using RADIUS authentication. The RADIUS client on the SMC forwards the RADIUS message to a single or multiple RADIUS servers configured for authentication. RADIUS authentication applies to both stand-alone and cluster configurations.

Procedure 53
Configuring the SMC for RADIUS support

1 Start a console terminal.

2 Press <Enter> on the console terminal to establish the connection.

Result: The SMC login prompt appears.

3 Enter **admin** for the default login name.

4 Enter **admin** for the default password.

5 Set a password.

   a. Enter **edit *xxxx***, where xxx represents the name of the user.

   b. Enter **password**.

   c. Enter the current admin password.

   d. Enter new password for the user.

   e. Reenter the password to confirm it.

   Note: The RADIUS server must have the same username and password that was configured in the CLI.

6 Enter **apply** to apply the changes.

7 Configure the RADIUS server.

   a. Enter **/cfg/sys/adm/auth/servers**.

   b. Enter **add**.

   c. Enter ***nn.nn.nn.nn***, where nn.nn.nn.nn is the RADIUS IP address.

   d. Choose one of the following:

      — Enter the port number.

      — Press <Enter> to accept the default.

   e. Enter the shared secret value of the RADIUS server.

8 Enter **`ena`** to enable RADIUS authentication.

9 Enter **`apply`** to apply the configuration.

End of Procedure

You can set the RADIUS server up in an HA configuration. The console session in the current master takes over and login is possible through the console and the Web UI. If failover occurs, the web session can log off and you must authenticate again.

Web User Interface (UI)

Contents

This chapter contains information about the following topics:

Introduction

This section explains how to enable the Web User Interface (UI), configure your web browser, and launch the Web UI to access the Secure Multimedia Controller (SMC) system-management features from your web browser.

Characteristics of the Web UI

Following are the characteristics of the Web UI:

- installation not required; the Web UI is part of the SMC operating system (OS) software
- upgrades with future software releases (as available)
- accessible through HTTP, or secure HTTPS using Secure Socket Layer (SSL)
- provides an intuitive user interface structure
- provides configuration and monitoring functions similar to those available through the Command Line Interface (CLI)
- supports up to ten simultaneous Web UI sessions

Getting started

Following are the requirements to enable the Web UI:

- installed SMC
- PC or workstation with network access to the SMC host IP address
- frame-capable web browser software, such as the following:
  - Netscape Navigator 7.0 or higher
  - Internet Explorer 5.5 or higher
- JavaScript enabled in your web browser

  Note: JavaScript is not the same as Java. Ensure that JavaScript is enabled in your web browser.

End of Procedure

Using the VRRP virtual IP address to access the SMC Web UI

To use the VRRP virtual IP address to access the SMC using the Web UI, you must first enable management support for the VRRP interface.

Use the following CLI command to enable management support for the VRRP interface:

```
/cfg/net/if #/mgmt/ena/apply
```

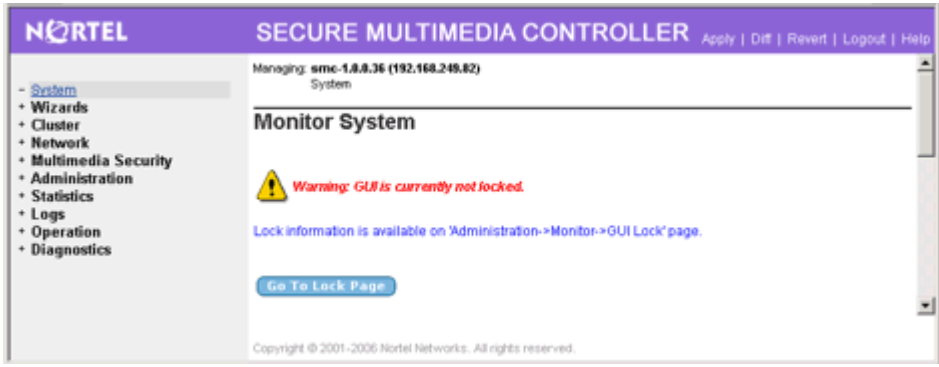
The virtual IP address is specified with the ip1 or ip2 command in the CLI menu.

Basics of the Web UI

Interface components

The SMC Web UI main page has eight component areas. See Figure 32 on page 203.

Figure 32
SMC Web UI main page



Main page tabs

Two main page tabs are available:

- **Wizards**: The Wizards tab provides access to wizards that guide users through the processes of initial configuration, interface and bridge addition, and routes and gateway configuration. To use the wizards, select **Initial Configuration**, **Add**, or **Configure**..., and follow the instructions on the screen. Click the plus sign (+) adjacent to a selection to expand it and reveal its associated sub-categories.
- **Config**: The Config tab is the default tab for the Web UI main page and provides access to all of the monitoring and configuration functions.

SMC Config main menu tree

Each of the selections on the Config main menu tree represents a page, called a form, which provides a method to monitor or configure the SMC.

Each main menu category offers sub-categories, providing a further level of control or detailed information. Click the plus sign (+) adjacent to a selection to expand it and reveal its associated sub-categories.

Warning display area

The Warning display area provides important warnings for the user, such as information about CLI users logged on or the status of the GUI lock. Any user

logged on as an administrator can activate the GUI lock before changing or creating a configuration.

IMPORTANT!

Lock the GUI before making changes.

Forms display area

The Forms display area contains fields that display information or allow you to specify information for configuring the system. The fields are different for each form.

Global command buttons

The global command buttons are always available at the top of each form. These commands summon forms used for:

- saving, examining, or canceling configuration changes
- logging out

Status icon

The Status icon for the SMC appears between the host IP address and cluster MIP. When the Status icon is green, the SMC is operating, and when the status icon is red, the SMC is offline.

Current alarms status

The Current alarms status provides the current status of all active alarms.

Basic operation

The SMC Web UI provides a variety of levels of control. To access the full functionality of the Web UI, you must log on as administrator.

The administration methods available in the Web UI are identified in Table 18.

Table 18
SMC administration

SMC function	Administration method
Create a configuration	Use the Config or Wizards tab
Submit form changes	Click the Update or Submit button on the form.
View pending changes	Click the global Diff button.
Clear pending changes	Click the global Revert button to cancel all pending changes.
Apply changes	Click the global Apply button.

Up to ten simultaneous Web UI sessions are allowed. When multiple CLI or Web UI sessions are open concurrently, only pending changes made during your current session are affected by use of the global Diff, Revert, or Logout commands. When multiple CLI or Web UI administrators apply changes to the same set of parameters concurrently, the latest applied changes take precedence.

WARNING

To prevent conflicts, any user logged on as administrator can take control of the GUI lock before changing or creating a configuration.

Pending change exceptions

After submission, most changes are considered pending and are not immediately put into effect or permanently saved. However, changes to users, passwords, and date or time zone take effect when the form is submitted.

Lost changes

Changes are lost if a new form is selected or the session is ended without submitting the information to the pending configuration. Click the **Update** or **Submit** button on the form to submit changes to the pending configuration.

Pending changes are also discarded if they are not submitted before the inactivity timeout value on Web UI sessions elapses. The Web UI inactivity timeout value is five minutes and cannot be changed.

Global command forms

The global command buttons are always available at the top of each form.

These buttons display forms used to save, examine, or cancel configuration changes, and log off. Each global command form provides options to verify or cancel the command.

Apply

Use the global Apply form to check the validity of the pending configuration changes for the current session, and to save the configuration changes and put them into effect.

The global Apply form includes the following items:

- Apply Changes pull-down list: to use this menu, select one of the following commands and click the **Submit** button:
  - — Apply Changes: When selected, this command updates the SMC with any pending configuration changes. Pending changes are first validated for correctness. If no problems are found, the changes are applied and put into effect. If problems are found, applicable warning and error messages are displayed. Warnings are allowed, and the changes are applied and put into effect. Errors are not allowed, and the changes are not applied. This command has no effect on pending changes in other open CLI or Web UI sessions. See Figure 32 on page 203 for information about taking control of the GUI lock.
  - — Validate Configuration: When selected, this option validates pending changes for the current session, but does not apply them. The pending configuration changes are examined to ensure that they are complete and consistent. If problems are found, the following types of messages are displayed:

  - Warnings are in yellow. Warnings identify conditions to consider, but which do not cause errors or prevent configuration application.
  - Errors are in red. Errors identify serious configuration problems that require correction. Uncorrected errors cause the Apply Changes command to fail. If the configuration is valid, select Apply Changes and click Submit to apply the changes.

— Run a Security Audit: When selected, this command lists security information. Security information includes the status for remote management features such as Telnet, SSH, and the Web UI for the cluster. The IP addresses that access the remote management features are also listed. The Run Security Audit command also lists users configured with default passwords that require change.

- Submit button: Click to perform the action selected in the Apply Changes pull-down list.
- Back button: Click to return to the previously viewed form without applying changes.

Diff

The global Diff form provides a list of the pending configuration changes for the current session.

The list displays a change record for each submitted update. Each record can consist of many modifications, depending upon the complexity of the form and changes submitted. Modifications are color coded as follows:

- Green: New items that are added to the configuration after the global Apply command is given and verified.
- Blue: Existing items to be modified.
- Red: Configuration items to be deleted.

The Diff list is cleared when configuration changes are applied or reverted, or when you log off or close the browser window.

Note: The Diff form does not include pending changes made in other concurrent CLI or Web UI sessions.

Revert

Use the global Revert form to cancel pending configuration changes.

The global Revert form includes the following items:

- Revert button: Click the Revert button to cancel the pending configuration changes for the current session. TIP: Applied changes are not affected. Pending changes made in other open CLI or Web UI sessions are not affected. See Figure 32 on page 203, Administration/ Monitor/GUI Lock form. To prevent conflicts, any user logged on as administrator can take control of the GUI lock before changing or creating a configuration.
- Back button: Click the Back button to return to the previously viewed form without canceling pending changes.

Logout

Use the global Logout form to terminate the current user session.

The global Logout form includes the following items:

- Logout button: Click the Logout button to terminate the current user session. TIP: Any un-applied configuration changes made during this session that are lost. This command has no effect on pending changes in other open CLI or Web UI sessions.
- Back button: Click the Back button to return to the previously viewed form without logging out.

The context-sensitive Help window consists of the following areas:

- Sub-page menu: Click Pages to display Help for the selected form. Click Tasks to activate the task-based Help system.
- Help topic menu: Select a new Help topic using the menu on the left side of the Help window. Each main menu item is listed, along with the sub-menu items under the current selection. Select a different menu item to display its sub-menu list. Select any sub-menu item to display Help for that form.
- Load: Click Load to display the form referenced on the bar.

- Forms area: This area displays detailed information about the selected topic.
- Close button: Click Close to close the context-sensitive Help window.

Task-based Help

Task-based Help directs the administrator through the steps of various common procedures. To access task-based Help, click the global Help button and then click the Tasks bar. The task Help menu appears in a new window with information appropriate for the current Web UI form (see Figure 33 on page 210):

Figure 33
Task Help menu

The task-based Help window consists of the following areas:

- Sub-page menu: Click Pages to display Help for the selected form. Click Tasks to activate the task-based Help system (see Figure 33 on page 210).
- Task topic menu: Select from a list of tasks using the menu on the left side of the Help window. Each main task item is listed, along with the sub-tasks under the current selection. Select a different sub-task to reveal the steps required to complete it.
- Forms area: This area displays the steps required to complete the selected sub-task.
- Load Page link: Click Load Page to display the form referenced on the task topic menu. If the sub-task has more than one step, the steps are listed on the form.
- Click .. to display the information for the next sub-task.
- Click ..: to display the information for the previous sub-task.
- Close button: Click Close to close the task-based Help window.

Logging

Contents

This chapter contains information about the following topics:

Introduction

The SMC has an extensive logging infrastructure, which includes three primary types of logs: system, security, and UNIStim. This chapter discusses each type of log file and details how logging can potentially become a performance bottleneck and provides ways to avoid this bottleneck.

Log types

System Log

The System Log contains general device-level status information and errors. You can view the contents of the System Log in the Web UI at the **Logs > System Log** page.

Note: Many System Log messages have Log IDs, such as LIBADMIN_32 or USECPD_16. In the Web UI log display page, you can search on these IDs and show additional information about the log message (and possible resolutions).

Security Log

The Security Log displays attack and packet-level information, including potential exploits and problem packets, logged from the SMC firewall. You can view the Security log in the Web UI at the **Logs > Security Log** page. Because the Security Log can log a message for every packet, it can quickly become a performance bottleneck.

IMPORTANT!

The Security Log can degrade SMC performance if it logs too many messages. See “Security log rate-limiting” on page 215 for more information about limiting the system effects of this log.

UNIStim log

The UNIStim Log contains basic UNIStim security information and errors generated by the Secure UNIStim proxy. You can view the UNIStim log in the Web UI at the **Logs > UNIStim Proxy Log** page.

Log configuration

Remote logging

You can configure the System Log and the Security Log messages to forward to a remote system log server in real-time. To limit the amount of traffic, you can also configure a filter to trap for System Log messages by the message priority parameter. Configure Remote logging in the Web UI at the **Cluster > Logs** page.

Log archiving

Because logs can potentially become large and consume too much disk space, you can configure the SMC to rotate the logs either when they reach a certain

size or after a specific interval of time. After log rotation, the logs are e-mailed to the specified external system. You can individually configure each of the different log types, depending upon expected log volume.

Security log rate-limiting

The security log has the greatest risk of becoming large and/or consuming significant system resources. This can occur, for example, if a log message is generated for every packet that transmits to the SMC. To limit this risk, the SMC provides various levels of control over the number of generated log messages and their rate.

Features

Limit by message type

In the Web UI at the **Multimedia Security > Security Settings > Log > Messages** page, you can enable or disable logging for certain types of messages such as particular attacks, globally allowed packets, and globally denied packets.

IMPORTANT!

Logging for Unavailable Policies (that is, generating a log message for any traffic that does not match an existing policy) is disabled by default, because it has the potential of generating many messages in a new installation; however, logging for Unavailable Policies messages are helpful when debugging network communication problems by logging packets that are silently dropped by the firewall.

Limit by count

You can specify that logging only occurs for a limited number of messages in a given period of time. Limiting by count prevents the CPU from becoming over-used in managing log resources. However, it provides an inaccurate report of the state of the current system because log messages beyond the limit are dropped.

Limit by sampling

The SMC supports logging every nth message (for example, storing 1 out of every 10 messages). Limiting by sampling has the same problem as the previous option (not all messages are logged). However, because it uses sampling large blocks of messages are not discarded.

Logging thresholds

For better performance, you can configure the SMC firewall to buffer log messages before storing them; however, expect a delay between when the log is created and when the log is committed to disk. This delay can cause difficulties when troubleshooting in real-time.

Policy-based logging

You can enable or disable logging for each firewall policy. If enabled, all packets that match that policy generate a log message.

Security Log details

This section contains information about two aspects of using the log: the concept of self policies, and rule ID mappings. For information about Security Log details, see “SMC packet filter log messages” on page 259.

Self policies

The SMC has multiple levels of protection, such as self policies, for traffic addressed to itself. Self policies are included in the standard firewall rule base; these policies cannot be modified. Self policies can trap for certain messages and then send details to the Security Log.

Rule id mappings

Firewall log messages often map to a specific firewall rule, as defined by a rule ID listed in the log. An example follows:

```
Apr 29 20:06:48 172.16.7.225 id=firewall time="2004-04-29
14:49:48" fw= a10-10-10-10 pri=1 proto=6(tcp)
src=172.16.8.226 dst=172.16.7.224 mid=2077 mtp=128
```

```
msg="Deny access policy matched, dropping packet Src 45121
Dst 21 from ext n/w" ruleid=23 agent=Firewall
```

The mapping of rules to log messages is dynamic. Using the **Diagnostics > Applied Rules** page in the Web UI, you can map a particular rule ID to the type of traffic. You can view inbound, outbound, and self rules generated on this page.

Note: Adding a UNIStim server adds rules to the database as well. These rules are called autogenerated rules and are displayed in green on the rule mappings page.

Limits and Scaling

Contents

This section contains information about the following topics:

Configuration limits

Parameter	Limit
Secure Multimedia Zones	4
Networks	512
Services	512
Flows	32
Keys	8
UNIStim Policies	64
UNIStim Rules	512
UNIStim Servers	32
Firewall Rules	1024

Firewall limits

Parameter	Limit
Connections	700,000 across all zones

Engineering limitations

Because the hardware is a PC platform, small packet performance can be a limitation for high-end systems. The hardware provides at least 100 Mbps (Megabits per second) throughput for 128 byte packets or approximately 100,000 pps (100 Kpps) in each direction, with essentially zero packet loss. This throughput is sufficient to support approximately 1000 concurrent calls, assuming 50-100 pps/call in each direction.

It is important to note that this applies to packet traversal across the SMC, and in both directions (200 Mbps bidirectionally). In a typical deployment, call signaling is much less than 100 Mbps in each direction but the packet sizes

are typically much smaller. It is possible to have RTP media traversing across the SMC at these bandwidths if IP phones communicate from one zone to another. In these cases, 100 Mbps of 128 byte packet size RTP media can traverse the SMC, bidirectionally, with zero percent packet loss. In addition, extended tests with peak 110 Mbps inflow + 40 Mbps outflow (150Mbps bidirectionally) with typical RTP codecs are run. PSQM and RTP media statistics are within acceptable limits.

Some of the typical codecs included the following:

- G.711u 20ms (approximately 214 byte packet size)
- G.711u 10ms (approximately 134 byte packet size)

Secure UNIStim limitations

Secure UNIStim limitations primarily deal with both secure UNIStim connection rate (connections per second) and secure UNIStim concurrent session load and capacity.

The secure UNIStim connection rate limitations are necessary to handle the CPU-intensive full RSA handshakes. If incoming secure UNIStim connections are above a certain limit, connections are dropped due to CPU over-utilization and SMC latency. If the sessions have a master key cached on the SMC, the full RSA handshake can be bypassed and the successful rate of incoming UNIStim connections increase accordingly. The SMC is tested for approximately 27 *non-cached* incoming connections/second. An SMC is able to support this connection rate with little or no loss in client registrations. In a VRRP scenario, the master keys are synchronized to the backup (that is, the master keys are cached on the backup SMC). The 27 connection rate per second is supported with no loss in client re-registration during a failover, given that the master keys in this scenario is already cached.

Secure UNIStim and general UNIStim proxy limitations include generic limitations of the UNIStim process itself. The UNIStim proxy process threads can be tied up (attacked) if packets are forged and sent at very high rates (several Mbps). Note that these rates far exceed the rates that the UNIStim proxy is required to handle in a typical deployment. To “protect” the UNIStim proxy a full variety of rate limiting settings are available under the /maint/

unistim/adv/flow menu. The UNIStim proxy is not designed to accommodate tens of Mbps of UNIStim control traffic.

Scaling beyond 5000 clients

The maximum license for an SMC device is 5000 Secure UNIStim users. To support installations with requirements beyond 5000 users, load balancing of UNIStim traffic is required.

Appendix A: Troubleshooting

Contents

This appendix contains information about the following topics:

VRRP/HA connectivity troubleshooting

If VRRP configuration is added and enabled or an SMC is added to the cluster but not responding, perform the following:

1. Check the cabling and that all the ports have link/traffic LED indication as expected.
2. Log onto the initial SMC by the console.
3. Ping the initial SMC to the interface and Virtual IP addresses of the initial SMC.
4. Ping the initial SMC to the gateway IP address on the intranet.
5. Ping the initial SMC to the interface IP addresses on the second SMC. This assumes that the networks are connected through the Layer 2 device.

Security error and fingerprint update issues

During the initial Secure UNIStim deployment, `Security Error` is a common error message seen on the IP Phone screen.

The cause of this error is typically the mismatch of the fingerprints. That is, the currently configured IP Phone fingerprint does not match either the primary or secondary fingerprint.

For more information about fingerprints, see “Managing the keys” on page 151.

To prevent this error, ensure the fingerprint on the IP Phone matches either the primary or the secondary fingerprint on the SMC. If the fingerprints do not match, further action may be required depending on how the IP Phone is currently configured as identified in Table 19 on page 225

Table 19
Fingerprint update troubleshooting

IP Phone configuration	Action
IP Phone has preconfigured fingerprint	If the IP Phone is running secure UNIStim previously, it may have a fingerprint already configured which is different from both the current SMC primary key and secondary key configurations. To correct this error, manually delete the old fingerprint and enter the new fingerprint on the IP Phone.
IP Phone has empty fingerprint or `FFFFFFFFFFFFFFFF` as the fingerprint and prefers auto-assignment	To configure the SMC to assign the correct fingerprint to this IP Phone, perform the following steps: **1** On the IP Phone, set the Action Byte to 1 for non-secure mode. **2** On the SMC, configure a client policy default policy with the following rules: Upgrade = y, Security = y, and fprint = y. **3** Connect the IP Phone to the Call Server through the SMC. During the connection handshake, the SMC writes a new fingerprint to the IP Phone and upgrades the IP Phone to secure UNIStim mode.
Automatic fingerprint update	To update the primary RSA key and assign the corresponding new fingerprint to all the IP Phones, perform the following steps during a maintenance window: **1** On the SMC, assign the current primary RSA key to the secondary key. This ensures that IP Phones with the old fingerprint can still register securely. **2** Generate a new RSA key and attach it as the Primary RSA key. The SMC automatically writes the new fingerprint to all the registered IP Phones.

Server Unreachable error

Unsecure clients that reside in the same subnet as Secure UNIStim clients can fail if the SMC policy requires clients from this subnet to run Secure UNIStim. The failed clients receives a `Service Unreachable` error message.

To resolve this error, change SMC policy to Upgrade = y and Security = n. Then the policy upgrades clients with secure capabilities to run secure UNIStim and lets clients without secure UNIStim capabilities to run insecure mode even though these clients are mixed together in the same subnet.

Appendix B: Regulatory information

Contents

This appendix contains information about the following topics:

System approval

The Secure Multimedia Controller (SMC) has approvals to be sold in many global markets. The regulatory labels on the back of system equipment contain national and international regulatory information.

Electromagnetic compatibility

The system meets Class A Electromagnetic compatibility (EMC) requirements for all countries.

WARNING

In a domestic environment, the system can cause radio interference. In this case, the user can be required to take adequate measures.

Table 20 describes the EMC specifications for Class A devices:

Table 20
EMC specification for Class A devices

Jurisdiction	Standard	Description
United States	FCC CFR 47 Par 15	FCC Rules for Radio Frequency Devices (See Note 1 on page 229)
Canada	ICES-003	Interference-causing equipment. Radio disturbance characteristics. Limits and methods of measurement. (See Note 3 on page 229)
Europe	EN 55022/ CISPR 22	Information technology equipment. Radio disturbance characteristics. Limits and methods of measurement. (See Note 3 on page 229)
	EN 55024	Information technology equipment. Immunity characteristics. Limits and methods of measurement.
	EN 6100-3-2	Limits for harmonic current emissions (equipment input current < = 16 A per phase).
	EN 6100-3-3-	Limitation of voltage fluctuations and flicker in low-voltage supply systems for equipment with rated current < = 16 A per phase.
Australia	CISPR 22/ AS/NZS 3548	Limits and methods of measurement of radio disturbance characteristics of information technology equipment. (See Note 3 on page 229)
Korea	KN22	Information technology equipment. Radio disturbance characteristics. Limits and methods of measurement.
	KN24	Information technology equipment. Immunity characteristics. Limits and methods of measurement.
Taiwan	CNS 13438	Limits and methods of measurement of radio disturbance characteristics of information technology equipment.

Note 3: FCC CFR 47 Part 15.21 statement:
"Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, can cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense."

Note 4: The user should not make changes or modifications not expressly approved by Nortel. Any such changes can void the user's authority to operate the equipment.

Note 5: EN 55022/CISPR 22 Statement:
"Warning
This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

DenAn regulatory notice for Japan

取扱説明書

安全上のご注意

本取扱説明書「安全上のご注意」は以下のノーテル製品の取扱説明書の別紙であり、取扱説明書本文と不可分のものです。

- Communication Server 1000M Cabinet/Chassis
- Communication Server 1000S
- Communication Server 1000E
- Meridian 1 Option 11C
- Meridian 1 Option 11C Mini
- Media Gateway 1000
- Multimedia Communication Server 5100
- CallPilot 703t server
- Hospitality Messaging Server 400
- Media Processing Server 500
- Media Processing Server 1000

⚠ 警告

本製品を安全にご使用頂くため、以下のことにご注意ください。

- 接続ケーブル、電源コード、ACアダプタなどの部品は、必ず製品に同梱されております添付品または指定品をご使用ください。添付品・指定品以外の部品をご使用になると故障や動作不良、火災の原因となることがあります。
- 同梱されております付属の電源コードを他の機器には使用しないでください。上記注意事項を守らないと、死亡や大怪我など人身事故の原因となることがあります。

ノーテルネットワークス株式会社
〒141－0032 東京都品川区大崎1丁目11番2号
ゲートシティ大崎イーストタワー9F
TEL: 03-5740-1300 (代表)
http://www.nortel.com/jp

Appendix C: Specifications

Contents

This appendix contains information about the following topics:

Hardware and power supply specifications

Table 21 lists hardware specifications for each characteristic of the SMC.

Table 21
Hardware specifications

Characteristic	Measurement
Chassis format	1U high custom base chassis
Motherboard	Custom Network Engines motherboard
CPU	Intel Pentium-4, 2.8 GHz, 533MHz FSB
Chipset	ServerWorks GC-SL
Memory	512 MB DDR 200/266MHz, ECC Registered; motherboard supports up to 4GB total
LAN ports	(2) 10/100/1000Base-TX (copper) ports on the motherboard
Expansion Slots	(2) Full-height 64-bit 133/100/66MHz PCI-X slots

Table 21
Hardware specifications (Continued)

Characteristic	Measurement
PCI Card	(1) Intel Dual Port Copper 10/100/1000 Base-TX GB-E IDE PCI card PWLA8492MT
Serial Port	(1) Console port, DCE (DB9-F), RS-232C, 9600 Baud, 8-N-1
USB Port	(2) USB 1.1 ports
Drives	(1) 40GB or 80GB IDE hard drive, 7200 RPM, ATA133, size depends on market availability (1) CD-ROM 24X slim-profile, optional support for one floppy drive (not presently installed)
System Management	CPU temperature/voltage monitoring, fan monitoring
System LEDs	Power (green) HDD activity (green) System status (amber) — CPU fans 1-4 — system fans — +5V, +12V — CPU temperature — motherboard ambient temperature
Power Supply	300W, 100-240VAC, 50-60Hz Power consumption: 125W typical BTU: 429 BTU/hr average
Operating Conditions	Temperature: 5-35 degrees C, 10%-90% humidity (non-condensing) Shock: 0-5G half sine, 2 ms
Non-operating Conditions	Temperature: -20-80 degrees C, 10%-90% humidity (non-condensing) Shock: 0-50G half sine, 2 ms
Acoustic Noise	35 DBA

Table 21
Hardware specifications (Continued)

Characteristic	Measurement
MTBF	Greater than 50,000 hrs
Rack mountable	Rack mount hardware to allow mounting in 19 inch standard rack
Bezel	plastic front bezel with Nortel name/logo and SMC 2450 model name and number
Physical Dimensions	1U high, 19 inch rack width, 22 inch depth
Weight	approximately 25 pounds
Regulatory	Safety: — UL 60950, CSA 22.2 No 60950, EN60950, IEC60950 Emissions: — FCC Part 15 Class A, Canada ICES-003 Class A — EN55022 (emissions) Class A and EN55024 (immunity) — CISPR-22, VCCI, AS/NZ 3548 Certification Marks: — cULus, CE, FCC PART 15, Gost, NOM, S-Mark, TUV-GS, MIC ***Note:*** The system is qualified with the above certifications, additional scans will need to be performed to qualify the Quad GigE PCI card with the system.

LAN connection speeds

Table 22 lists LAN connection speeds accommodated by the SMC.

Table 22
LAN connection speeds

LAN connection speed	Connector	Medium
10BaseT	RJ-45	CAT3, CAT4, or CAT5 UTP
100BaseTX	RJ-45	CAT5 UTP
1000BaseT	RJ-45	CAT5 UTP

Regulatory specifications

Table 23 lists safety specifications. Table 24 on page 234 lists emissions specifications. Table 25 on page 235 lists certification marks.

Table 23
Safety specifications

Compliance	Country
UL60950	USA
CSA22.2 No 60950	Canada
EN60950	Europe
IEC60950	Europe

Table 24
Emissions specifications

Compliance	Country
FCC Part 15 Class A	USA
Canada ICES-003 Class A	Canada

Table 24
Emissions specifications (Continued)

Compliance	Country
AS/NZ 3548	Australia & New Zealand (standard replaced by EN55022)
EN55022 (emissions) & EN55024 (immunity)	Europe
CISPR-22	Europe
VCCI	Japan

Table 25
Certification marks

Compliance	Country
cULus	USA & Canada
CE	Europe
Gost	Russia
NOM	Mexico
S-Mark	Argentina
TUV-GS	Germany/Europe
MIC	Korea

Appendix D: Software licenses

The SMC includes software that is covered by the following licenses:

Apache Software Licence

The Apache Software License, Version 1.1

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1 Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3 The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

"This product includes software developed by the Apache Software Foundation (http://www.apache.org/)."

Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4 The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5 Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information about the Apache Software Foundation, please see <http://www.apache.org/>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

mod_ssl License

LICENSE

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1 Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3 All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

4 The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.

5 Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.

6 Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenSSL and SSLeay Licenses

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2001 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1 Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3 All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4 The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5 Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6 Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1 Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3 All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.

4 If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Brian Gladman's License

Copyright (c) 2002, Dr Brian Gladman <brg@gladman.me.uk>, Worcester, UK. All rights reserved.

LICENSE TERMS

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;

2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;

3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

ALTERNATIVELY, provided that this notice is retained in full, this product may be distributed under the terms of the GNU General Public License (GPL), in which case the provisions of the GPL apply INSTEAD OF those given above.

DISCLAIMER This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose.

Issue Date: 26/08/2003

Peter Gutmann's License

/* The random pool handling code in this module and the misc/rnd*.c modules represent the cryptlib continuously seeded pseudorandom number

generator (CSPRNG) as described in my 1998 Usenix Security Symposium paper "The generation of practically strong random numbers".

The CSPRNG code is copyright Peter Gutmann (and various others) 1995-2002 all rights reserved. Redistribution of the CSPRNG modules and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice and this permission notice in its entirety.

2. Redistributions in binary form must reproduce the copyright notice in the documentation and/or other materials provided with the distribution.

3. A copy of any bugfixes or enhancements made must be provided to the author, <pgut001@cs.auckland.ac.nz> to allow them to be added to the baseline version of the code.

ALTERNATIVELY, the code may be distributed under the terms of the GNU General Public License, version 2 or any later version published by the Free Software Foundation, in which case the provisions of the GNU GPL are required INSTEAD OF the above restrictions.

Although not required under the terms of the GPL, it would still be nice if you could make any changes available to the author to allow a consistent code base to be maintained */

PHP License

The PHP License, version 2.02

Copyright (c) 1999, 2000 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1 Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3 The name "PHP" must not be used to endorse or promote products derived from this software without prior permission from the PHP Group. This does not apply to add-on libraries or tools that work in conjunction with PHP. In such a case the PHP name may be used to indicate that the product supports PHP.

4 The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number.

Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.

5 Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes PHP, freely available from http://www.php.net".

6 The software incorporates the Zend Engine, a product of Zend Technologies, Ltd. ("Zend"). The Zend Engine is licensed to the PHP Association (pursuant to a grant from Zend that can be found at http://www.php.net/license/ZendGrant/) for distribution to you under this license agreement, only as a part of PHP. In the event that you separate the Zend Engine (or any portion thereof) from the rest of the software, or modify the Zend Engine, or any portion thereof, your use of the separated or modified Zend Engine software shall not be governed by this license, and instead shall be governed by the license set forth at http://www.zend.com/license/ZendLicense/.

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the PHP Group.

The PHP Group can be contacted via Email at group@php.net.

For more information on the PHP Group and the PHP project, please see <http://www.php.net>.

SMTPclient License

LICENSE

SMTPclient—simple SMTP client

Copyright (C) 1997 Ralf S. Engelschall, All Rights Reserved.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of

MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License in the file COPYING along with this program; if not, write to:

Free Software Foundation, Inc.,
675 Mass Ave, Cambridge,
MA 02139, USA.

Notice, that “free software” addresses the fact that this program is **distributed** under the term of the GNU General Public License and because of this, it can be redistributed and modified under the conditions of this license, but the software remains **copyrighted** by the author. Don't intermix this with the general meaning of Public Domain software or such a derivated distribution label.

The author reserves the right to distribute following releases of this program under different conditions or license agreements.

Ralf S. Engelschall
rse@engelschall.com
www.engelschall.com

GNU General Public License

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended

to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1 This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

2 Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

3 You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

4 You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

5 You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for non-commercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

6 You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

7 You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

8 Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

9 If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims;

this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

10 If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

11 The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

12 If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

13 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

14 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion

of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

> <one line to give the program's name and a brief idea of what it does.>
> Copyright (C) 19yy <name of author>
>
> This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.
>
> This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.
>
> You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

> Gnomovision version 69, Copyright (C) 19yy name of author
> Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type ‘show w’.
> This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands ‘show w’ and ‘show c’ should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ‘show w’ and ‘show c’; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

> Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' written by James Programmer.
>
> <signature of Official>, 1 April 1989
> Official, Title

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Appendix E: SMC packet filter log messages

Contents

This appendix contains information about the following topics:

Format

SMC firewall logs use the industry standard Webtrends Extended Log Format (WELF) for logging network activity. A sample of a log message in WELF generated by syslog is shown here.

```
Apr 18 04:25:52 172.16.1.247 id=firewall time="2002-04-18
16:15:34" fw=DEVICE1 pri=6 proto=6(tcp) src=172.16.7.246
dst=66.218.70.149 msg=Service access request successful
Src 3171 Dst 80 from EXT n/w agent=Firewall
```

Various fields in the above sample syslog message are explained in Table 26:

Table 26
Syslog message fields

Field	Description
Syslog header	Contains the time stamp of the event.
Id	Identifies the type of record.
time	Shows the date and time of the event, in terms of local time.
fw	Identifies the SMC that generated the log record.
pri	Identifies the priority of the event.
proto	Identifies the protocol used by the event.
Src	Identifies the IP address that generated the event.
dst	Identifies the IP address that received the event.
msg	Shows the detailed log message based on the event.
agent	Shows the name of agent generating log message.

Log message table

Table 27: “Log messages” on page 261 describes log messages generated by SMC. It also specifies the log category of the respective event.

Table 27
Log messages

Default Enable Category	
System Boot Complete	This log message is generated when the system start-up procedure is complete. `Wed Jun 23 17:15:10 2004 id=firewall time="2004-06-23 17:11:23" fw=a10-10-10-10 pri=6 mid=450 mtp=0 msg="Device Boot/Initialise procedure completed" agent=Firewall`
System Error Messages	
Resource Limit Reached	This log message indicates that respective direction's connection table to be reached, and no additional connections can be made in that direction. `Apr 29 20:07:53 172.16.7.225 id=firewall time="2004-04-29 14:50:53" fw= a10-10-10-10 pri=1 proto=6(tcp) src=172.16.8.226 dst=172.16.7.224 mid=2080 mtp=2048 msg="Rate-Limiting: Max Connection Limit reached Src 45127 Dst 23 from ext n/w" ruleid=27 agent=Firewall`
Maximum Packet Rate Reached	This log message indicates that the maximum packet rate is reached and no extra packets are allowed. `Apr 29 19:53:28 172.16.7.225 id=firewall time="2004-04-29 14:36:28" fw= a10-10-10-10 pri=1 mid=2102 mtp=2048 msg="Rate-Limiting: Maximum Packet Rate reached, dropping the packet from ext n/w" ruleid=23 agent=Firewall`

Table 27
Log messages

Maximum Connection Rate Reached	This log message indicates that the maximum connection rate is reached and new connections within that rate limiting time are not formed. `Apr 29 20:09:20 172.16.7.225 id=firewall time="2004-04-29 14:52:19" fw= a10-10-10-10 pri=1 proto=6(tcp) src=172.16.8.226 dst=172.16.7.224 mid=2079 mtp=2048 msg="Rate-Limiting: Max Connection Rate reached Src 45132 Ds 21 from ext n/w" ruleid=27 agent=Firewall`
Maximum Bandwidth Reached	This log message indicates that the maximum bandwidth to pass is reached and further packets are dropped. `Apr 29 19:52:41 172.16.7.225 id=firewall time="2004-04-29 14:35:41" fw= a10-10-10-10 pri=1 mid=2103 mtp=2048 msg="Rate-Limiting: Maximum Bandwidth Reached, dropping the packet from ext n/w" ruleid=23 agent=Firewall`
Deny Policies	
Deny Policy Matched	This log message is generated when the respective traffic is permitted to traverse the SMC. `Apr 29 20:06:48 172.16.7.225 id=firewall time="2004-04-29 14:49:48" fw= a10-10-10-10 pri=1 proto=6(tcp) src=172.16.8.226 dst=172.16.7.224 mid=2077 mtp=128 msg="Deny access policy matched, dropping packet Src 45121 Dst 21 from ext n/w" ruleid=23 agent=Firewall`

Table 27
Log messages

Allow Policies	
Allow Policy Matched	This log message is generated when the respective traffic is permitted to traverse the SMC. `Apr 29 20:07:13 172.16.7.225 id=firewall time="2004-04-29 14:50:13" fw= a10-10-10-10 pri=6 proto=6(tcp) src=172.16.8.226 dst=172.16.8.225 mid=2030 mtp=256 msg="Service access request successful Src 45122 Dst 80 from ext n/w" ruleid=3 agent=Firewall`
Unavailable Policies	
Access Policy Not Found	This log message is generated when there is no policy configured for the packet to traverse the SMC. `Apr 29 20:14:11 172.16.7.225 id=firewall time="2004-04-29 14:57:11" fw= a10-10-10-10 pri=4 proto=6(tcp) src=172.16.8.226 dst=172.16.8.225 mid=2076 mtp=4096 msg="Access Policy not found, dropping packet Src 45134 Dst 21 from ext n/w" agent=Firewall`
SynFlood Attack	
Flooding	This log message is generated when the association table grows beyond 80 percent of its limit, and SMC activates TCP SYN Flooding protection. `Apr 29 20:30:04 172.16.7.225 id=firewall time="2004-04-29 15:13:03" fw= a10-10-10-10 pri=1 proto=6(tcp) src=172.16.7.224 dst=172.16.8.226 mid=2066 mtp=1 msg="Crossed 80% of resource. Possible flooding(TCP) Src 1048 Dst 23 from corp n/w" agent=Firewall`

Table 27
Log messages

General attacks	
LAND	This log message is generated when the SMC detects a land attack. `Apr 29 17:46:16 172.16.7.225 id=firewall time="2004-04-29 12:29:15" fw= a10-10-10-10 pri=1 proto=6(tcp) src=172.16.7.224 dst=172.16.7.224 count=1 mid=2000 mtp=2048 msg="Possible Land Attack detected. Src 23 Dst 23 from ext n/w" agent=Firewall`
Unable to Determine Route	This log message is generated when the SMC is unable to determine a route to the source. `Apr 29 21:36:10 172.16.7.225 id=firewall time="2004-04-29 16:19:10" fw= a10-10-10-10 pri=1 proto=197 src=89.128.155.52 dst=172.16.7.224 mid=2031 mtp=2048 msg="Unable to find route for source, from ext n/w" agent=Firewall`
IP-Reassembly	This log message is generated when the SMC detects possible IP-Reassembly attack. `Apr 15 03:58:38 172.16.1.249 id=firewall time="2002-04-15 15:40:09" fw= a10-10-10-10 pri=1 proto=1(icmp) src=172.16.2.244 dst=172.16.1.5 msg=IpReasmbly Fragment count exceeds max limit from EXT network agent=Firewall`
IP-Source Route Options	This log message is generated when source routing option is set in IP Datagram. `May 6 17:20:17 172.16.1.151 id=firewall time="2002-05-06 17:13:27" fw= a10-10-10-10 pri=1 proto=17(udp) src=172.16.2.150 dst=172.16.1.150 msg=Source routing option set in IP packet from EXT n/w agent=Firewall`

Table 27
Log messages

IP-Reassembly Timeout	This log message is generated when the SMC detects possible IP-Reassembly attack. `Apr 29 21:08:38 172.16.7.225 id=firewall time="2004-04-29 15:51:38" fw= a10-10-10-10 pri=6 proto=6(tcp) src=172.16.8.226 dst=172.16.7.224 mid=10 mtp=0 msg="IpReassembly time out" agent=Firewall SNetName=Internet`
Data Inspection	
Invalid Sequence Number	This log message is generated when the SMC detects an invalid sequence number. `Apr 15 05:23:31 172.16.1.250 id=firewall time="2002-04-15 17:04:45" fw= a10-10-10-10 pri=1 proto=6(tcp) src=172.16.2.244 dst=172.16.2.249 msg=Invalid sequence number received with Reset, dropping packet Src 1089 Dst 23 from EXT n/w agent=Firewall`
Invalid TCP Connection	This log message is generated when the SMC detects an invalid TCP connection. `Apr 29 21:27:55 172.16.7.225 id=firewall time="2004-04-29 16:10:55" fw= a10-10-10-10 pri=1 proto=6(tcp) src=172.16.7.224 dst=172.16.8.226 count=9 mid=2002 mtp=2048 msg="Invalid TCP Connection request Src 23 Dst 2058 from corp n/w" agent=Firewall`

Table 27
Log messages

IP Spoof	
IP Spoof	This log message is generated when the SMC detects and IP-Spoof attack. `Apr 15 03:30:32 172.16.1.249 id=firewall time="2002-04-15 15:12:10" fw= a10-10-10-10 pri=1 proto=1(icmp) src=172.16.1.249 dst=172.16.255.255 msg=ICMP Type: 8 Code:0 Spoofing detected, dropping packet from EXT n/w agent=Firewall`
Ping of Death	
Ping of Death	This log message is generated when the SMC detects a Ping of death attack. `Apr 15 05:01:59 172.16.1.250 id=firewall time="2002-04-15 16:43:17" fw= a10-10-10-10 pri=1 proto=1(icmp) src=172.16.1.142 dst=172.16.2.249 msg=Ping of Death attack detected from CORP n/w agent=Firewall`
IP Option Attacks	
IP Option Attack	This log message is generated when the SMC detects invalid IP options in a packet. `Apr 3 15:40:04 172.16.1.152 id=firewall time="2004-03-03 15:40:04" fw= a10-10-10-10 pri=5 proto=6(tcp) src=172.16.1.152 dst=172.16.1.163 msg=Invalid IP options, dropping packet from CORP n/w agent=Firewall`

Table 27
Log messages

Winuke	
Winnuke	This log message is generated when the SMC detects a Winnuke attack. `Apr 30 11:06:41 172.16.7.225 id=firewall time="2004-04-30 05:49:42" fw= a10-10-10-10 pri=1 proto=6(tcp) src=172.16.8.226 dst=172.16.7.224 mid=2020 mtp=16 msg="Terminating connection as WinNuke Attack detected, OOB packet Src 45310 Dst 21 from ext n/w" ruleid=31 agent=Firewall`
Access Statistics	
Connection Closed	This log message is generated when a connection is closed. `Apr 29 19:43:08 172.16.7.225 id=firewall time="2004-04-29 14:26:08" fw= a10-10-10-10 pri=6 proto=6(tcp) src=172.16.8.226 dst=172.16.8.225 mid=2086 mtp=32768 msg="Connection closed.Bytes transferred : 22837 Src 36636 Dst 80 from ext n/w" ruleid=3 agent=Firewall`
Connection Terminated	This log message is generated when a connection is terminated. `Apr 29 20:43:26 172.16.7.225 id=firewall time="2004-04-29 15:26:26" fw= a10-10-10-10 pri=6 proto=6(tcp) src=172.16.7.224 dst=172.16.8.226 mid=2087 mtp=32768 msg="Connection terminated.Bytes transferred : 232 Src 1051 Dst 23 from corp n/w" ruleid=28 agent=Firewall`
Connection Timed Out	This log message is generated when a connection times out. `Apr 29 20:44:40 172.16.7.225 id=firewall time="2004-04-29 15:27:40" fw= a10-10-10-10 pri=6 proto=17(udp) src=172.16.7.225 dst=172.16.7.224 mid=2088 mtp=32768 msg="Connection timed out.Bytes transferred : 6554 Src 32777 Dst 514 from self n/w" ruleid=12 agent=Firewall`

Appendix F: SMC 1.0 Autogenerated rules

Contents

This appendix lists the SMC autogenerated rules, which are created when the SMC is first configured, or generated later in CLI or Web UI wizards.

WARNING: Application Gateway TLAN rules require that HTTP be opened for general users. This allows the HTTP protocol into the TLAN, where it also can be used to access Element Manager (which is a security issue).

Recommendation: You should disable the Application Gateway rules in the TLAN if they are not in use, or configure the TLAN without the Application Gateway using the Automatic Rule Generation Wizard in the Web UI:

Multimedia Security > Security Zones > zone name > Automatic Rule Generation

ELAN

Table 28
Services

Name	Port(s)	Protocol	Description
ftp	21	tcp	File transfer protocol
telnet	23	tcp	Telnet
http	80	tcp	HTTP protocol
snmp	161-162	udp	SNMP query
rlogin	513	tcp	Rlogin protocol

Table 29
Inbound rules

Source	Destination	Service	Comment
administrators	zone	ftp	ELAN File Transfer Protocol
administrators	zone	telnet	ELAN Telnet
administrators	zone	http	ELAN Element Management
administrators	zone	rlogin	ELAN Rlogin
administrators	zone	1929 (UDP)	ELAN Database Admin for OTM
administrators	zone	5001, 5002 (UDP)	ELAN Call Server SNMP
administrators	zone	snmp	ELAN SNMP

TLAN

Table 30
Services

Name	Port(s)	Protocol	Description
ftp	21	tcp	File transfer protocol
telnet	23	tcp	Telnet
tftp	69	udp	Trivial file transfer protocol
http	80	tcp	HTTP protocol
snmp	161-162	udp	SNMP query
https	443	tcp	HTTPS protocol
rlogin	513	tcp	Rlogin protocol

Table 30
Services

Name	Port(s)	Protocol	Description
UNIStim_cs1000	4100, 5100, 7300	udp	UNIStim signaling for CS 1000
sip_tcp	5060	tcp	SIP TCP signaling
sip_udp	5060	udp	SIP UDP signaling

Table 31
Inbound rules

Source	Destination	Service	Comment
administrators	zone	ftp	TLAN FTP
administrators	zone	telnet	TLAN Telnet
administrators	zone	http	TLAN Element Management
administrators	zone	rlogin	TLAN Rlogin
administrators	zone	snmp	TLAN SNMP
users	zone	1720 (TCP)	TLAN H.323 TCP Signaling
users	zone	1718-1719 (UDP)	TLAN H.323 UDP Signaling
users	zone	sip_tcp	TLAN SIP TCP Signaling
users	zone	sip_udp	TLAN SIP UDP Signaling
users	zone	tftp	TLAN Trivial File Transfer Protocol
users	zone	UNIStim_cs1000	TLAN i200x UNIStim Signaling
users	zone	5105 (UDP)	TLAN i200x UNIStim FTP
users	zone	10000 (UDP)	TLAN Port Mapping Discovery
users	zone	12800 (TCP)	TLAN Remote Office Signaling

Table 31
Inbound rules

Source	Destination	Service	Comment
users	zone	16500-16501 (TCP)	TLAN Virtual Office Signaling
users	zone	16500-16501 (UDP)	TLAN Virtual Office Signaling
users	zone	20480 (UDP)	TLAN Remote Office RTP
users	zone	20482 (UDP)	TLAN Remote Office RTP
users	zone	SVP	TLAN SVP Wireless Protocol

TLAN – Application Gateway

Table 32
Services

Name	Port(s)	Protocol	Description
http	80	tcp	HTTP protocol
https	443	tcp	HTTPS protocol

Table 33
Inbound rules

Source	Destination	Service	Comment
administrators	zone	http	Application Gateway HTTP
administrators	zone	9001 (TCP)	Application Gateway Administration Tool (HTTPS)
administrators	zone	9005 (TCP)	Application Gateway Design Studio Configuration

Table 33
Inbound rules

Source	Destination	Service	Comment
administrators	zone	9014 (TCP)	Application Gateway Cluster Communication (HTTP)
administrators	zone	9025 (TCP)	Application Gateway Cluster Communication (HTTP)
users	zone	5000 (UDP)	Application Gateway UNIStim Signaling
users	zone	50005 (UDP)	Application Gateway RTCP Receive
users	zone	44443 (TCP)	Application Gateway GXAS Service
users	zone	http	Application Gateway Broadcast Server Push
users	zone	20480-20511 (UDP)	Application Gateway / Remote Gateway Audio
users	zone	https	Application Gateway Smart A

SLAN – Call Pilot

Table 34
Services

Name	Port(s)	Protocol	Description
ssh	22	tcp	SSH protocol
ftp	21	tcp	FTP protocol
http	80	tcp	HTTP protocol
smtp	25	tcp	SMTP protocol

Table 34
Services

Name	Port(s)	Protocol	Description
imap2	143	tcp	IMAP2 protocol
snmp	161-162	udp	SNMP protocol
ldap	389	tcp	LDAP protocol
https	443	tcp	HTTPS protocol
ssmtp	465	tcp	Secure SMTP
ldapssl	636	tcp	LDAP over SSL

Table 35
Inbound rules

Source	Destination	Service	Comment
users	zone	20 (TCP)	CallPilot Application Builder FTP
users	zone	ftp	CallPilot FTP
users	zone	smtp	CallPilot SMTP
users	zone	http	CallPilot HTTP Element Management
users	zone	135 (UDP)	CallPilot Location Service
users	zone	135 (TCP)	CallPilot Location Service
users	zone	137 (UDP)	CallPilot NETBIOS
users	zone	137-139 (TCP)	CallPilot NETBIOS
users	zone	imap2	CallPilot IMAP2
administrators	zone	snmp	CallPilot SNMP
users	zone	ldap	CallPilot LDAP

Table 35
Inbound rules

Source	Destination	Service	Comment
users	zone	https	CallPilot HTTPS
users	zone	ssmtp	CallPilot Secure SMTP
users	zone	ldapssl	CallPilot LDAP over SSL
users	zone	993 (TCP)	CallPilot Application Builder IMAP
users	zone	1025-1026 (TCP)	CallPilot msdtc
users	zone	1027-1028 (TCP)	CallPilot Microsoft Distribute COM
users	zone	1029-1032 (TCP)	CallPilot Dialogic CTMS
users	zone	1036 (TCP)	CallPilot Middleware Maintenance Service
users	zone	1037 (TCP)	CallPilot Call Channel Resource
users	zone	1038 (TCP)	CallPilot Multimedia Resource
users	zone	1039-1041 (TCP)	CallPilot MCE Notification Service
users	zone	1042 (TCP)	CallPilot MTA
users	zone	1045 (TCP)	CallPilot Access Protocol
users	zone	1046 (TCP)	CallPilot SLEE
users	zone	1047-1048 (TCP)	CallPilot IIS
users	zone	1095-1096 (TCP)	CallPilot Blue Call Router
users	zone	1148 (TCP)	CallPilot TAPI
users	zone	1499 (TCP)	CallPilot Reporting ODBC
users	zone	2019-2020 (TCP)	CallPilot Dialogic CTMS
users	zone	5631 (TCP)	CallPilot pcAnyware Data
users	zone	5632 (UDP)	CallPilot pcAnyware Stat
users	zone	7934 (TCP)	CallPilot IIS

Table 35
Inbound rules

Source	Destination	Service	Comment
users	zone	8000 (TCP)	CallPilot Dialogic CTMS
users	zone	10008 (TCP)	CallPilot Access Protocol
users	zone	38037 (TCP)	CallPilot msgsys Intel CBA-Message System
users	zone	56325 (TCP)	CallPilot SLEE

SLAN – Contact Center/Symposium

Table 36
Services

Name	Port(s)	Protocol	Description
snmp	161-162	udp	SNMP protocol

Table 37
Inbound rules

Source	Destination	Service	Comment
administrators	zone	snmp	Symposium SNMP
administrators	zone	1550 (TCP)	Symposium HDX CAPI
administrators	zone	3000 (TCP)	Symposium MSLM (MLink)
administrators	zone	4422 (TCP)	Symposium HDX Name Service
administrators	zone	5000-5003 (TCP)	Symposium SQL Server
administrators	zone	5631 (TCP)	Symposium pcAnywhere
administrators	zone	5632 (UDP)	Symposium pcAnywhere

Table 37
Inbound rules

Source	Destination	Service	Comment
elan	zone	8888 (TCP)	Symposium AML Communication
Note: AML communication is disabled by default. If needed, it should be enabled by the user after the ELAN network has been set appropriately.			

SLAN – OTM/TM

Table 38
Services

Name	Port(s)	Protocol	Description
http	80	tcp	HTTP protocol
https	443	tcp	HTTPS protocol

Table 39
Inbound rules

Source	Destination	Service	Comment
administrators	zone	http	OTM Web Client HTTP
administrators	zone	https	OTM Web Client HTTPS
administrators	zone	4789-5045 (TCP)	OTM Web Client Virtual System Terminal
administrators	zone	135 (TCP)	OTM Windows Client Login
administrators	zone	135 (UDP)	OTM Windows Client Login
administrators	zone	139 (TCP)	OTM Windows Client NetBEUI File Sharing

Table 39
Inbound rules

Source	Destination	Service	Comment
administrators	zone	1583 (TCP)	OTM Windows Client Btrieve Station Administration
administrators	zone	3351 (TCP)	OTM Windows Client Btrieve Station Administration
administrators	zone	162 (UDP)	OTM SNMP Traps
administrators	zone	1929 (UDP)	OTM DBA Configuration
administrators	zone	1930-1939 (UDP)	OTM DBA Signalling
administrators	zone	2176-2185 (UDP)	OTM DBA Data
administrators	zone	5099 (TCP)	OTM RMI OTMDECT

MCS 5100

Table 40
Services

Name	Port(s)	Protocol	Description
ssh	22	tcp	SSH protocol
http	80	tcp	HTTP protocol
https	443	tcp	HTTPS protocol
UNIStim_mcs	5000	udp	i200x UNIStim signaling for MCS
sip_udp	5060	udp	SIP UDP signaling

Table 40
Services

Name	Port(s)	Protocol	Description
mcs_lom	2100, 2200, 2300, 2400, 2500, 2600, 2700, 2800	tcp	Terminal server LOM
mcs_serial	3100, 3200, 3300, 3400, 3500, 3600, 3700, 3800	tcp	Terminal server serial

Table 41
Inbound rules

Source	Destination	Service	Comment
administrators	zone	http	MCS HTTP Element Management
administrators	zone	https	MCS HTTPS Element Management
administrators	zone	ssh	MCS SSH
administrators	zone	11111 (TCP)	MCS Management Console
administrators	zone	5631 (TCP)	MCS PcAnyWhere (TCP)
administrators	zone	5632 (UDP)	MCS PcAnyWhere (UDP)
administrators	zone	3389 (TCP)	MCS Windows Terminal Services
administrators	zone	3339 (TCP)	MCS HTTP Provisioning
administrators	zone	5040 (TCP)	MCS Terminal Server
administrators	zone	mcs_lom	MCS Terminal Server LOM
administrators	zone	mcs_serial	MCS Terminal Server Serial
administrators	zone	3900 (TCP)	MCS Terminal Server SMDI
users	zone	http	MCS Personal Agent and Web Client

Table 41
Inbound rules

Source	Destination	Service	Comment
users	zone	sip_udp	MCS Session Initiation Protocol
users	zone	UNIStim_mcs	MCS UNIStim protocol for i200x phones
users	zone	1719 (UDP)	MCS H.323 Gatekeeper RAS
users	zone	1720 (TCP)	MCS H.323 Gatekeeper H.225
users	zone	50020 (UDP)	MCS i2004 firmware download
users	zone	3090 (TCP)	MCS WCM Session Control Protocol

Additional Product-Specific Rule Configuration

Besides the baseline rules added when the SMC is configured, extra configuration may be necessary for individual features. These additional configurations are listed below.

Table 42
Additional Product-Specific Rule Configuration

Feature	Notes
Symposium Multicast	Symposium uses multicast to send Real Time Data (RTD) to the Symposium Web Client (SWC) Server, and the SWC Server uses multicast to send RTD to Web Clients. To allow these multicast packets to traverse the SMC, a multicast bypass must be created. This can be done in the Web UI using a wizard or by adding the bypass directly: • Multicast Wizard: — Web UI: Wizards > Symposium Multicast • Multicast Bypass — Web UI: Multimedia Security > Security Settings > Multicast Bypass — CLI: /cfg/smc/settings/multicast
Symposium Contact Center – Manager	In Contact Center – Manager, if both ELAN and Server LAN are connected to the SMC, an additional rule needs to be enabled in the Server LAN inbound rule list to allow AML traffic to flow between the ELAN and the Server LAN.
CallPilot Desktop Messaging	CallPilot Desktop Messaging requires ICMP packets to be exchanged between the Desktop Messaging Client and the CallPilot Server. A wizard is provided to help configure this exchange, as well as to provide flow control: Web UI: Wizards > Firewall > CallPilot Desktop Messaging

Table 42
Additional Product-Specific Rule Configuration

Feature	Notes
CallPilot Application Builder	This product requires two large port ranges be opened for DCOM traffic: • 1024-65525 (UDP) • 1024-65535 (TCP) This is not currently done in the CallPilot autogenerated rules because it poses a security risk. If you are using Application Builder, add these ranges and limit the source network to only those who are using the application.
Optivity Telephony Manager/ Telephony Manager	Optivity Telephony Manager (OTM) requires that ICMP packets are exchanged between the OTM Standalone Server and the Call Server or ITG Card. SMC rule autogeneration does not include an explicit ICMP rule for these packets because it is a security hole. Instead, this support must be added manually using the OTM ICMP wizard: Wizards > Firewall > OTM ICMP
Server LAN	A firewall rule for Remote Desktop Agent (RDA) is not added by default to the Server LAN autogenerated rules. To add it manually, create an inbound rule for port 3389 (TCP).
RTP Portal	To add an MCS 5100 RTP Portal, a required rule for the RTP Portal must be added to the mcslan inbound rules if the RTP portal is on the mcslan. In most configurations, the RTP portal would be in a DMZ elsewhere on the network.

Secure Multimedia Controller 1.1

Fundamentals

Publication number: NN43001-325
Document release: Standard 02.01
Date: February 2009
Produced in Canada

To provide feedback or report a problem in this document, go to
www.nortel.com/documentfeedback

NORTEL